Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Vinícius Sondermann Martins Oliveira

EVOLUÇÃO DA TECNOLOGIA DE PROXY:
Analise de Características

Rio de Janeiro

2010

VINICIUS SONDERMANN MARTINS OLIVEIRA

EVOLUÇÃO DA TECNOLOGIA DE PROXY: Destaque de suas Características.

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Moacyr Henrique Cruz de Azevedo, M.Sc, UFRJ, Brasil

Rio de Janeiro

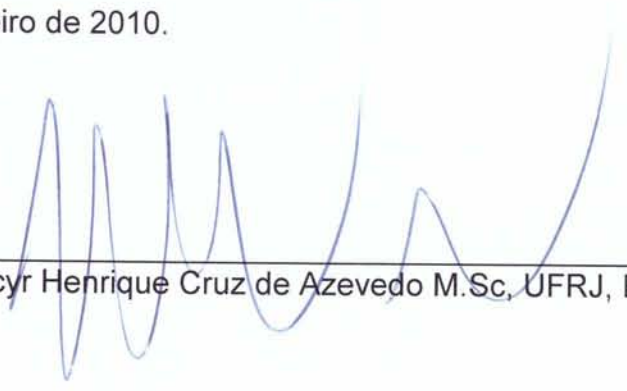
2010

Vinícius Sondermann Martins Oliveira

EVOLUÇÃO DA TECNOLOGIA DE PROXY: Destaque de suas Características.

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em fevereiro de 2010.



Moacyr Henrique Cruz de Azevedo M.Sc, UFRJ, Brasil

RESUMO

OLIVEIRA, Vinícius Sondermann Martins. **EVOLUÇÃO DA TECNOLOGIA DE PROXY: Destaque de suas Características**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2009.

Estudo realizado em três produtos largamente utilizados no mercado (Squid, Ironport e Blue Coat), com o intuito de descobrir como os Proxies (e seus caches) tratam o conteúdo dinâmico das paginas WEB e o quanto o cache local deste conteúdo permaneceria renovado em relação ao original na Internet.

Medições feitas a partir do hash de 13 amostras dos acessos a um site WEB de relevância nacional com conteúdo dinâmico, obtida em cada um dos três produtos foi comparada com o hash obtido do acesso direto sem intermediação de um Proxy.

Os resultados mostraram os diferentes comportamentos do cache de cada produto em relação ao conteúdo de sites dinâmicos, e que os produtos de software proprietário apresentaram vantagens em relação ao produto em software livre neste quesito.

ABSTRACT

OLIVEIRA, Vinícius Sondermann Martins. **EVOLUÇÃO DA TECNOLOGIA DE PROXY: Destaque de suas Características**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2009.

Research in three largely used products in the market (Squid, Ironport and Blue Coat), in order to understand how the proxies (and their caches) deal with the dynamic content of the web pages and how long the local cache of this content would be refreshed compared to its original in the Internet.

Measurements done by using 13 access samples to a web site of national relevance that contains dynamic content with the three products mentioned above were compared with the hash obtained from direct access without a proxy intermediation.

The results showed the different behaviors of the cache of each of the products in web dynamic content and what proprietary software products showed advantages when compared to free software.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Era muito comum confundirem o Proxy com firewall (em tempos distantes), pois o mesmo isolava a rede local do mundo externo. Porém, o Proxy não faz filtro de pacotes, apenas recebe o pedido, faz a busca e a entrega, enquanto o Firewall não vai buscar nada, apenas filtra o que está entrando e saindo.

O Proxy permitiu que em nossa rede local pudéssemos utilizar IPs privados e ter conectividade HTTP (posteriormente HTTPS) com a Internet sem precisar dispor de IPs públicos e, desta maneira ficamos menos vulneráveis.

1.1 PROBLEMA

Com o passar dos tempos os ataques se modificaram e as vulnerabilidades aumentaram. Mesmo que sua máquina não possua um IP público, ela continua vulnerável.

Pois as ameaças chegam por comunicações legitimas como e-mail e navegação WEB.

1.2 MOTIVAÇÕES

Hoje as empresas possuem uma visão de Gestão da Segurança da Informação e sabem que algumas informações são vitais para seus negócios, exigindo ferramentas que acompanhem a evolução das ameaças.

1.3 OBJETIVO

Mostrar a evolução tecnológica no que tange às novas funcionalidades do Proxy Corporativo e as diferentes abordagens dos fabricantes para tratarem a questão da Segurança da Informação.

1.4 ORGANIZAÇÃO DO TRABALHO

Este trabalho se divide em 5 partes, a primeira descreve sobre como funciona um Proxy, suas necessidades, funcionalidades nos dias atuais, e um teste prático com cache de Proxy em relação a sites de conteúdo dinâmico.

As partes seguintes abordam três produtos utilizados no mercado, sendo o primeiro software livre Squid e os dois restantes de tecnologias proprietárias Ironport e Blue Coat.

A última parte aborda alguns testes realizados em laboratório a respeito do tratamento do cache por estes produtos em relação a um site de conteúdo dinâmico.

2 PROXY - REFERENCIAL TEÓRICO

O Proxy é um serviço e como tal possui 2 funções. Funciona como um procurador ou representante porque todas as requisições WEB da rede local são feitas através dele, que se encarrega de ir buscar as informações no mundo externo (internet). Quando ele obtém as informações com sucesso, elas são entregues para o equipamento solicitante.

Outra função é a de cache WEB que significa que todas as informações recebidas , após serem encaminhadas ,ficam armazenadas localmente em disco, de forma que, quando outra requisição é recebida com o mesmo destino, o Proxy verifica se houve alteração de conteúdo e, caso não tenha ocorrido (ver Figura1), entrega a informação armazenada, agilizando a entrega desta informação e economizando uso do link para a Internet.

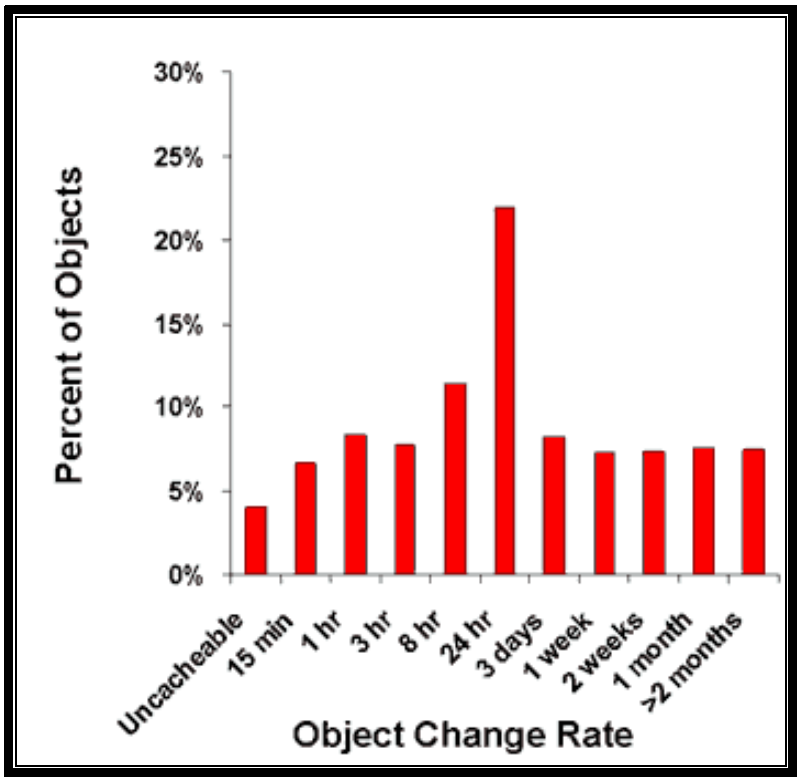


Figura 1 - Tempo médio de modificação de objetos WEB [2]

O Proxy é configurado no navegador a ser utilizado porém, é possível forçar os usuários a utilizarem o Proxy mesmo quando eles não configuram seus navegadores. A este método damos o nome de Proxy transparente, pois toda requisição feita à porta 80 do default gateway é ao Proxy, que se encarrega de fazer a solicitação externa e posterior entrega.

Com o uso corporativo da Internet, veio a necessidade de filtrar o que os usuários estão acessando de maneira que o tempo produtivo seja utilizado para assuntos pertinentes à atividades ligadas às empresas. Desta maneira os Proxy ganharam as listas de controle de acessos (ACLs) e foi possível definir o que poderia ser acessado permitindo classificação por grupo, individual e no tempo.

Podem ser definidas duas formas de acesso:

- Tudo é permitido por padrão e o que deve ser proibido é colocado em uma lista.
- Tudo é proibido por padrão e o que deve ser permitido é colocado em uma lista.

Com esta granularidade também foi possível implementar relatórios gerenciais que permitem o registro no mesmo nível de controle (o que, quem e quando) dado na permissão de acesso. Assim, foi resolvido o problema da queda de produtividade e também do uso racional dos recursos de rede da empresa (link internet).

Baseado nos relatórios de registros de acesso WEB, definiu-se que sites seriam classificados como proibidos e deveriam ser colocados em uma lista. Desta forma diariamente faz-se um levantamento dos sites acessados para definir o novo conteúdo permitido ou proibido. Com o número crescente de sites, isso se tornou uma tarefa árdua, quase impossível de ser mantida em ambientes de numerosos usuários.

O filtro de conteúdo WEB veio para melhorar bastante este cenário, pois desta forma as ACLs, ao invés de serem tratadas para cada site, passaram a ser tratadas por

categorias. Bastaria bloquear a categoria “esporte” e todos os sites de esportes que já estivessem cadastrados seriam bloqueados. O mesmo principio poderia ser usado para liberação de acesso.

Entretanto estas bases de dados, contendo os grupos e as urls respectivas, precisam ter manutenção constante devido ao alto número de inclusões e exclusões. O custo deste trabalho fez com que a maioria dos filtros de conteúdo para Proxy WEB fossem proprietários, embora existam soluções de software livre.

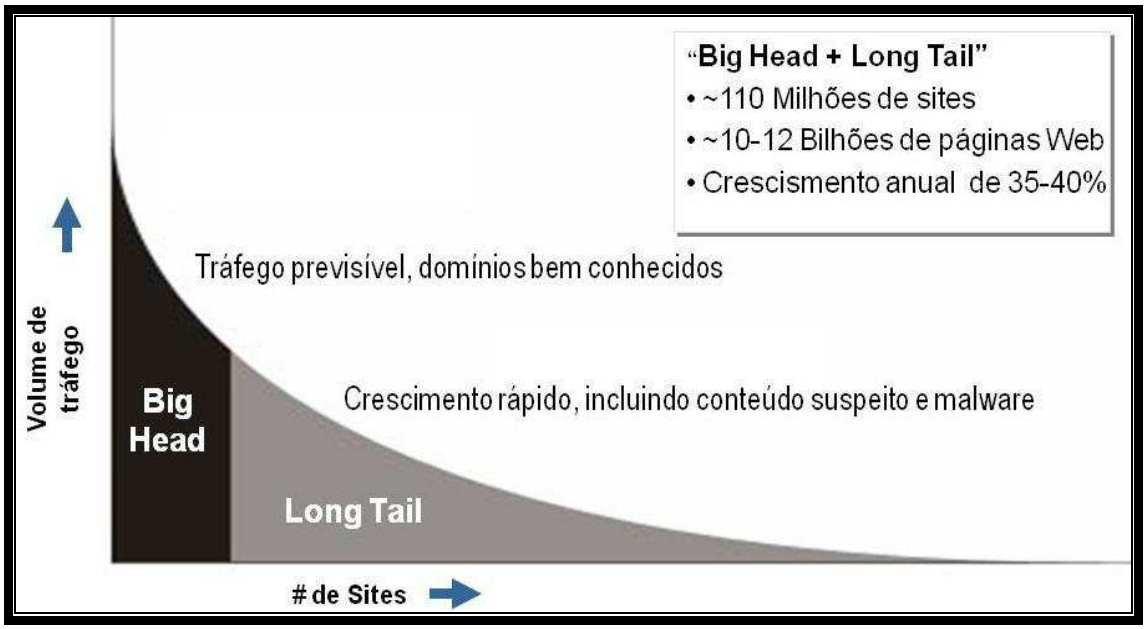


Figura 2 - Perfil do trafego WEB no mundo.

Os produtos de filtros de conteúdo normalmente são vendidos à parte para funcionar com diversos tipos de Proxy, sejam proprietários ou de software livre. Além da base são vendidas facilidades como interface para facilitar a aplicação de regras diversas, permissão de acesso, permissão de horário, acesso a conteúdo por extensão de nome de arquivo, acesso a arquivos do tipo mime (Extensões Multi função para Mensagens de Internet - é uma norma da internet para o formato das mensagens de correio eletrônico) de arquivo e etc.

Para registrar em logs e permitir ou negar acesso a nome de usuários ou grupos de usuários, foi preciso criar uma base local de usuários. Este método tornou-se de difícil gerenciamento em ambientes com muitos usuários, pois era necessário manter a base de acesso à rede local e a base de acesso à internet.

Desta maneira evolui-se para a autenticação dos usuários na base de dados de acesso à rede (o mais utilizado hoje é o Active Directory do Windows Server da Microsoft), e neste caso existem soluções de autenticação baseadas no Winbind do Samba, consultas LDAP (Lightweight Directory Access Protocol), e até mesmo agentes rodando em um servidor membro fazendo as requisições de autenticação pelo Proxy.

Figura 3 - Analise do Risco na WEB e custo com reparação do dano [5]

O serviço de redundância (fail over) se fez necessário para que não haja indisponibilidade do serviço ou, pelo menos deduzir o tempo em que ele fica indisponível (downtime). Com isto alguns Proxies implementaram o serviço de cluster, que poderiam ser ativo-ativo ou ativo-passivo. No ativo-ativo, além da disponibilidade que permite manter o serviço operando em caso de interrupção de

um dos Proxies, também ocorre balanceamento de carga. Já no ativo-passivo não existe este balanceamento de carga, apenas a disponibilidade do serviço.

A internet esta se tornando um ambiente cada vez mais hostil, dessa forma o Proxy se tornou mais um elemento da rede a ser protegido. O trafego HTTP inspecionado por antivírus (preferencialmente de fornecedor diferente do utilizado na rede, para aumentar o poder de proteção). Existem temos Proxy`s com antivírus integrados no mesmo equipamento e Proxies que utilizam equipamentos externos somente para esta função. Nesse último caso o Proxy se comunica com o equipamento antivírus através do protocolo ICAP (Internet Content Adaptation Protocol) que é utilizado para comunicação com antivírus). Se o servidor de antivírus da rede também utilizar o ICAP, o Proxy poderá utilizar este servidor de antivírus, embora isto possa aumentar significativamente o uso de CPU deste servidor.

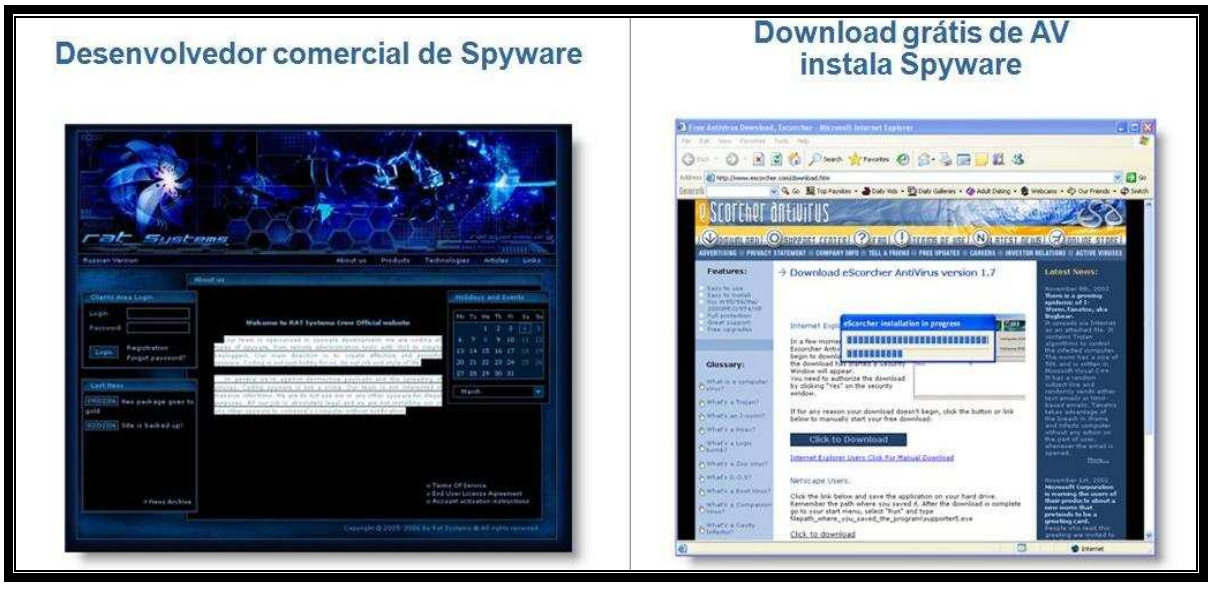


Figura 4 - Mercado Negro de Ferramentas de Espionagem.

Em ambientes com diversos sites é recomendado o uso de hierarquia de Proxy`s, cuja técnica permite economizar recursos de rede e agilizar as consultas WEB. Em

cada site remoto existe um Proxy filho e na matriz, onde está a conexão com a Internet, existe o Proxy Pai. Quando um usu[ario localizado em um site remoto faz uma solicitação, o Proxy filho verifica se possui a informação em seu cache e, se ela for válida, faz a entrega do conteúdo. Se a informação não for mais válida ou não estiver disponível, o Proxy filho encaminha a solicitação ao Proxy Pai que verifica em seu cache. Estando a informação disponível e válida, o Proxy Pai encaminha ao Proxy filho que por sua vez, atualiza o seu cachê e a encaminha ao usuário. Caso não tenha a informação o Proxy Pai vai buscá-la na Internet, atualiza seu cache e repassa ao Proxy filho.

Os Proxy`s mais modernos estão realizando a interceptação do protocolo SSL (Secure Socket Layer), agindo como intermediários. O cliente na rede local faz a solicitação ao Proxy que por sua vez, faz a solicitação ao site protegido. Porém ao invés de deixar o cliente fechar a conexão criptografada direto com o site protegido, o Proxy estabelece a conexão com o servidor remoto e “fingindo” ser o site remoto, estabelece outra conexão criptografada com o cliente na rede local. A conexão entre o cliente e o Proxy também fica criptografada, e o Proxy inspeciona o tráfego e repassa as informações da conexão cliente-Proxy para a conexão Proxy-servidor, atuando como “man in the midle”. Com esta medida pode-se aplicar políticas de segurança que impeçam a evasão de informações confidenciais relacionadas ao negócio da empresa. Outra finalidade dessa interceptação é verificar se os dados que entram na rede local estão infectados, uma vez que se a conexão está criptografada do servidor até o cliente, o Proxy fica impedido de varrer o conteúdo deste tráfego e detectar qualquer tipo de ameaça. Esta tecnologia será comentada mais adiante.

3 SQUID

O Squid derivou de um projeto chamado Harvest [7], foi desenvolvido inicialmente por universidades e centro de pesquisas dos Estados Unidos. Atualmente, porém, é desenvolvido por voluntários que construíram uma comunidade de desenvolvimento.

Junto com o Squid, outro projeto também derivou do Harvest. Chamado Netapp's Netcache, que foi adquirido pela Blue Coat em 2006.

O Squid tem código fonte aberto (é um software livre) e esta baseado na licença GPL. O Squid pode ser executado pelos seguintes sistemas operacionais: AIX, BSDI, Digital Unix, FreeBSD, HP-UX, IRIX, Linux, Mac OS X, NetBSD, NeXTStep, OpenBSD, SCO OpenServer, Solaris, UnixWare, Windows.

Precisar de suporte ao Squid não significa dificuldade por ele ser desenvolvido por voluntários em uma comunidade. Existem várias empresas que podem prestar suporte, conforme indicado no site http://www.squid-cache.org/Support/services.dyn

Com o Squid pode-se fazer o cache das páginas visitadas, acelerando a entrega do conteúdo HTTP e HTTPS.

Podemos fornecer autenticação centralizada por vários protocolos como módulos que podem utilizar os métodos PAM, SMB, LDAP e etc.

Algumas Características do Squid:

- Proxy e cache de protocolo HTTP, FTP;
- Proxy para SSL;
- Cache hierárquico;
- ICP, HTCP, CARP, Cache Digests;
- Cache Transparente;
- WCCP v1 e v2;
- Regras e Acesso e Conteúdo;

- Métodos de Autenticação;
- Aceleração para HTTP servers;
- Monitoramento SNMP;
- Cache de consultas DNS.

Além das características intrínsecas do Squid, podemos agregar funções ao mesmo acrescentando programas complementares que expandem em muito suas funcionalidades, tornado o Squid competitivo com algumas soluções proprietárias:

- SARG (Squid Analysis Report Generator)

  Ferramenta desenvolvida por um brasileiro, que utiliza o log access.log do Squid para gerar relatórios gerenciais sobre as estatísticas de acesso WEB de seus usuários. Por exemplo: Relatórios como sites mais acessados, quantidade de bytes entrando e saindo, sites bloqueados, falha de autenticação, sendo todos os registros com data e hora.

- Dansguardian

  É um filtro de conteúdo (software livre) que facilita muito o bloqueio de sites proibidos em ambientes de grande porte.

- Cache manager

  É um utilitário em formato CGI-bin que pode ser acessado via WEB para gerenciar o cache do Proxy sem precisar estar logado no sistema.

- Malware Block List

  Lista com urls contendo malwares que é atualizada diariamente em diversos formatos, sendo o formato de ACL’s do Squid um desses formatos.

O Squid é um Proxy largamente utilizado em todo planeta em virtude dos seus recursos aliados ao baixo custo. Tem um desenvolvimento amadurecido por muitos anos e uma gigantesca comunidade testando-o nos mais variados ambientes.

4 IRONPORT WEB SECURITY APPLIANCES

Figura 5 - IronPort WEB Security Appliances C-350.

A Ironport [2] atualmente é uma divisão da Cisco (comprada em janeiro de 2007). É uma empresa que se estabeleceu pelo sucesso de seu produto de segurança de emails e com seu revolucionário sistema de reputação por IP utlizando seu site senderbase.org (sistema também é utilizado pelo seu proxy WEB).

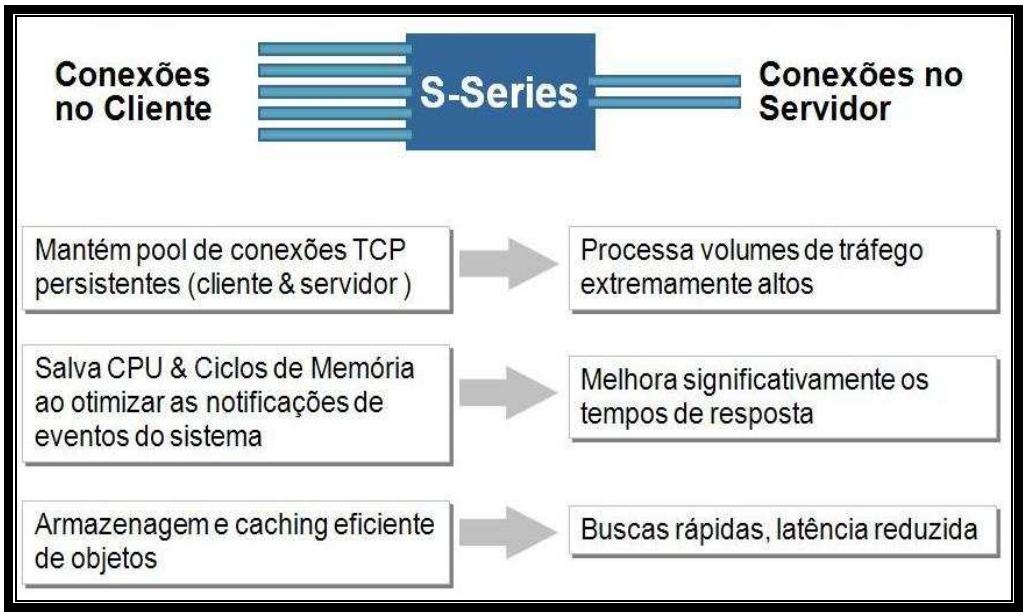


Figura 6 - Características da Arquitetura do Equipamento.

Seus equipamentos roda um sistema operacional denominado AsyncOS (versões diferentes para WEB e Email) que é uma modificação realizada baseada no Kernel do FreeBSD. Até mesmo sua pilha TCP/IP foi alterada para atender a elevada

demanda por conexões simultâneas (podendo um único equipamento aceitar 10.000 conexões simultâneas).

Os equipamentos de segurança WEB (Proxy) são denominados Series S e possuem alto desempenho. Contam com a exclusiva tecnologia de classificação de reputação e um novíssimo sistema de detecção chamado Dynamic Vectoring and Streaming (DVS), que faz filtragem de spyware baseado em assinatura durante o streaming dos dados. Possui ferramentas de Gerenciamento e Relatórios incluídas no próprio equipamento, são acessíveis via WEB e um equipamento em separado para administrar vários equipamentos simultaneamente de forma centralizada (IronPort Security Management Appliances).

Sistemas tradicionais não foram desenhados para os problemas de hoje:

- Orientados em torno de Cache, Autenticação e Controle de uso;
- Baixo throughput /alta latência;
- Baixa eficácia;
- Tempo de resposta lento;
- Visibilidade limitada.

Figura 7 - Comparativo com as arquiteturas mais comumente encontradas.

Os equipamentos Series S fazem a segurança em multicamadas do ambiente WEB contra spywares e diversas ameaças. É necessário fazer o adequado “sizing” da solução para não haver perda de performance.

Possui dois modelos:

- IronPort S650 – desenhado para corporações com as maiores demandas de trafego WEB do mundo – recomendado para organizações a partir de 5000 usuários.
- IronPort S350 – recomendado para organizações de até 5000 usuários.

Conexões TCP simultâneas	• 100,000 duplex	Processa picos significativos de tráfego
Transações HTTP/Hora	• 10M (unburdened) • 5M-7M (burdened)	Atende de 10-25K usuários (dependendo do volume de tráfego)
Latência média	• 5 a 15 millisegundos	Sem impacto na experiência de navegação do usuário

Figura 8 - Performance da Arquitetura.

Tendo um proxy de aplicação de alta performance, monitor de trafego Layer 4, e o mecanismo Dynamic Vectoring ans Streaming, consegue combinar desempenho e eficácia em um único equipamento.

Sua implantação pode ser feita nas seguintes configurações em relação à topologia:

- Em Linha: Proxy Transparente, agindo como uma Ponte Ethernet
- Desconectado (Offline): Sub-dividido em três tipos: Proxy Transparente, utilizando switch Camada 4; Proxy Transparente, através do WCCP do roteador; e Proxy de Redirecionamento Explicito.

Assim como nos equipamentos de Segurança de Email, a primeira camada de proteção é o filtro de classificação de reputação de ambientes WEB. Além de reduzir

as ameaças em um percentual significativo, este filtro também economiza banda ao impedir acesso a alguns sites e o download malwares.

Figura 9 - Quatro camadas de proteção.

4.1 SENDERBASE E FILTRO DE REPUTAÇÃO WEB

A primeira camada de proteção é o filtro de reputação, que é um filtro baseado no protocolo IP que exerce proteção do sistema WEB. Ele é um sistema simples que faz uma checagem local em caso de não haver nenhuma reputação definida no equipamento ele verifica uma base centralizada que é alimentada por todos os equipamentos da Ironport tanto de WEB quanto de e-mail.

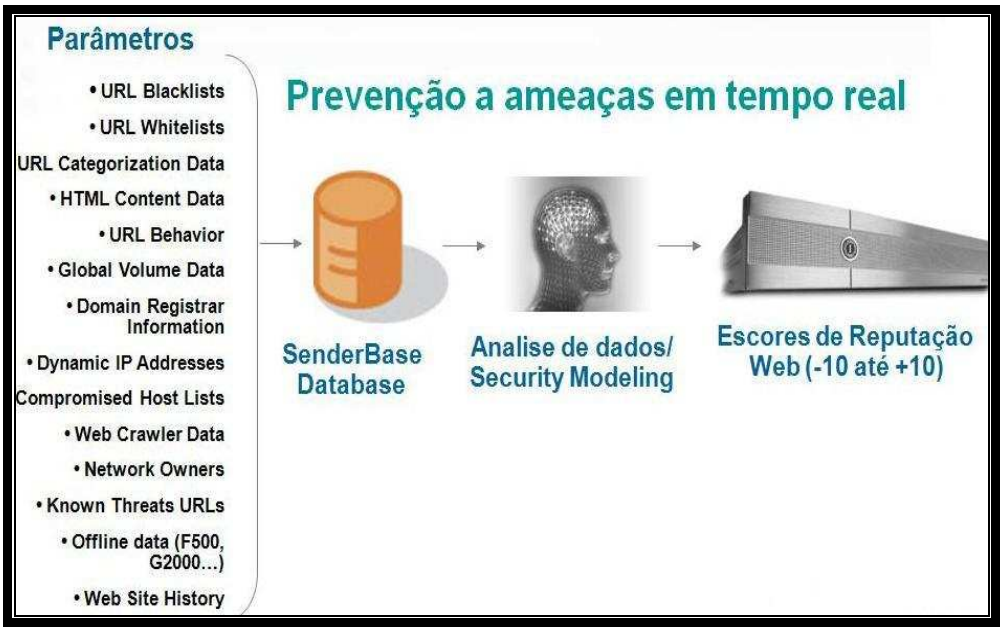


Figura 10 - Parâmetros utilizados para o calculo de pontuação da Reputação WEB.

Conforme a pontuação aplicada a um determinado site, o seu acesso será permitido ou não. Este processo consome quase nenhum processamento em relação às demais camadas de proteção, reduzindo significativamente o trafego a ser analisado pelas outras camadas, pois fica restando apenas o tráfego que foi aprovado pelo sistema de reputação.

O sistema de reputação WEB utiliza a mesma base da reputação por email, pontuando negativamente àqueles sites capturados dentro das mensagens de spam que foram localizadas dentro da rede de equipamentos de segurança de e-mails da Ironport.

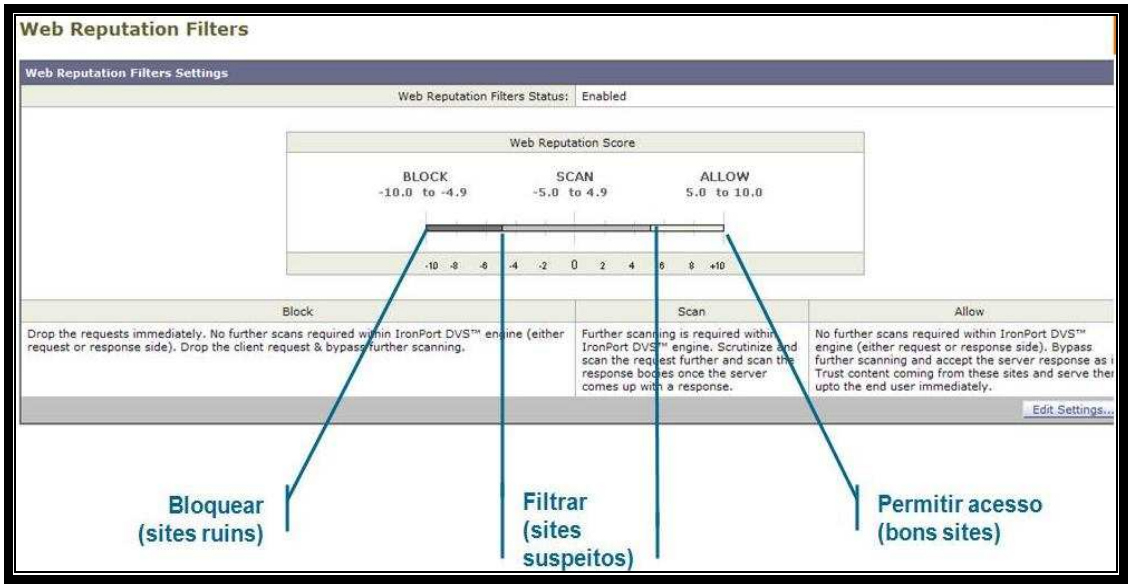


Figura 11 - Configuração do Bloqueio de Filtro de Reputação WEB (ver a pontuação -10 até 10).

Sabe-se que a grande maioria de spywares hoje é transmitida através de links que chegam através dos emails, com este sistema de pontuação negativa já ficam bloqueados na primeira camada de inspeção do equipamento de segurança WEB.

A Senderbase (www.senderbase.org) funciona como órgão fiscalizador criando um ranking (baseado em pontuação) para servidores de email e WEB. Esta base de

dados fica aberta para consulta via WEB, e conta com mais de 100.000 ISPs (Internet Service Providers), empresas e organizações que consultam e contribuem para sua atualização. Os equipamentos agem como sensores da rede em tempo real, alimentando essa base e se beneficiamndo ao fazer o download da base atualizada diariamente (como uma vacina de antivírus). Diversos critérios são utilizados pelos algoritmos que realizam os cálculos de pontuação (ver Fig. 11) que criam uma pontuação entre -10 e +10.

Com sensores instalados geograficamente em todos os pontos do planeta, é possível fazer análises geográficas do fluxo de acesso e de contaminações, apresentando uma visão em tempo real das ameaças em todo mundo.

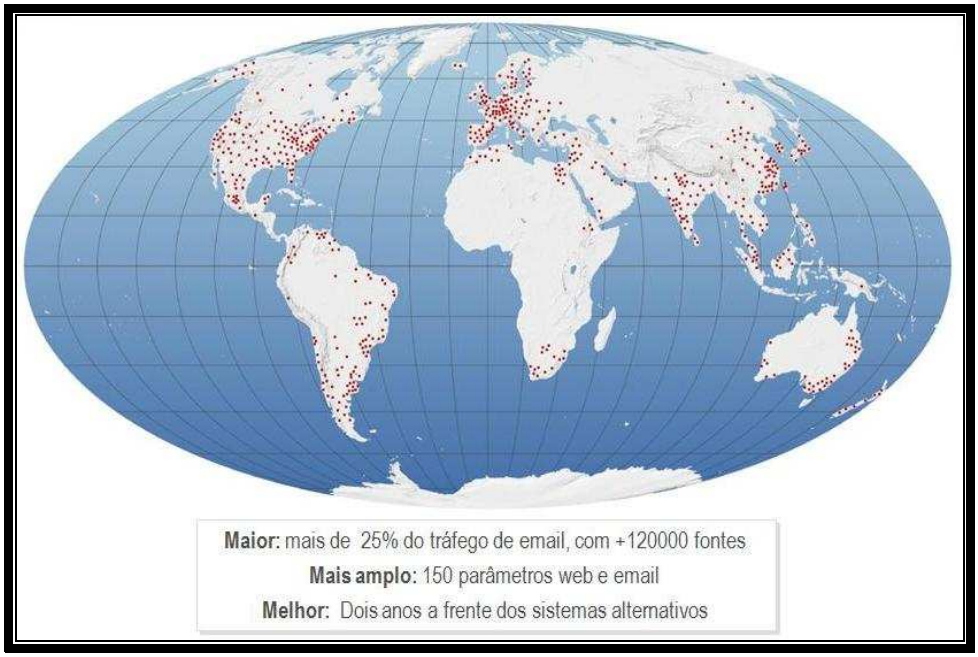


Figura 12 - Mapeamento Geográfico dos sensores que alimentam a Senderbase.

Após a consulta à Senderbase e coletada a pontuação de determinado site, três ações podem ocorrer: deixar passar sem varrer, varrer ou bloquear. Essas ações são feitas de acordo com faixas de pontos definidas pelo administrador e configuradas no equipamento.

Figura 13 - Esquema com o funcionamento do Filtro de Reputação WEB.

4.2 SISTEMA ANTI-MALWARE IRONPORT

- Inspeção de conteúdo completa e totalmente integrada;
- Maior eficácia contra uma grande variedade de ameaças;
- Performance sem igual;
- Baixo custo administrativo;
- Ampla cobertura;
- Combina o IronPort's DVS Engine com múltiplas ferramentas de filtragem;
- Atualmente suporta a ferramenta WEBroot.

Utiliza ferramenta da WEBroot que possui a maior e mais precisa base de dados de assinaturas anti-malware. Sobre ele pode-se dizer:

- Sistema automatizado de pesquisa de ameaças (Phileas);
- 240 vezes mais rápido que os métodos manuais;
- Ação proativa;
- Maior base de dados da indústria atuando sobre os diversos tipos de spywares : Adware, System Monitors, Pharming,Tracking Cookies, Browser Hijackers, Rootkits, Browser Helper Objects, Keyloggers, Trojans, Phishing;

- Aproximadamente 200 mil rastreamentos de malware;
- Equipe interna de pesquisa de ameaças aprimora e alimenta o banco de dados.

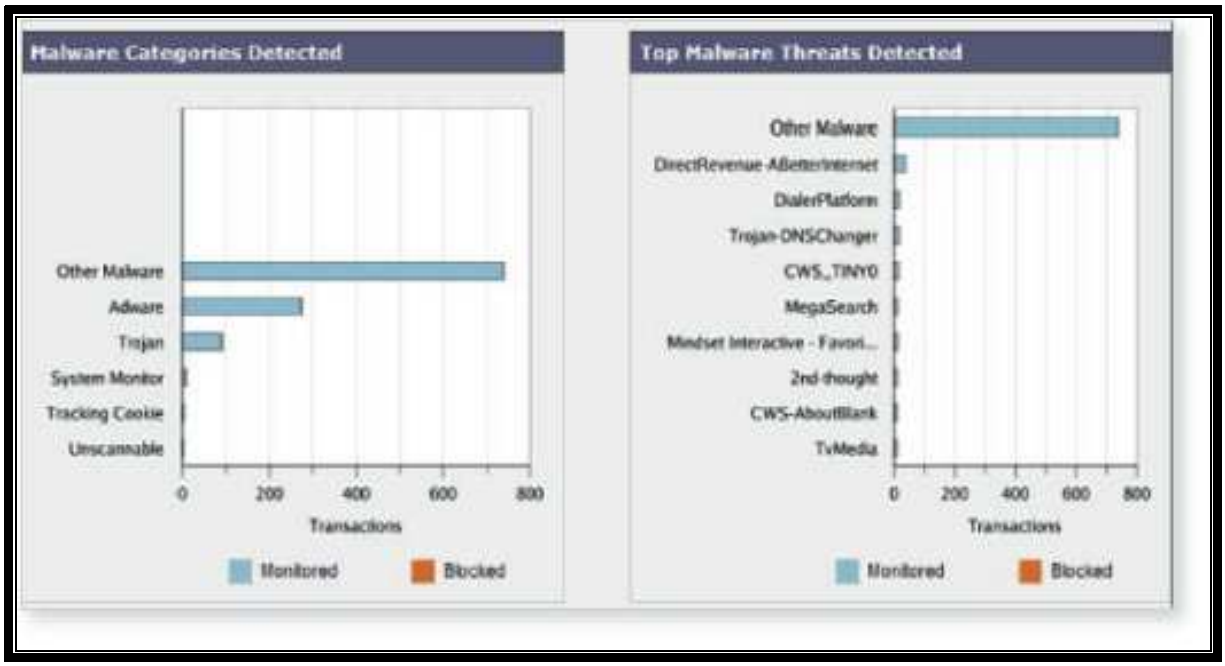


Figura 14 - Monitoramento em Tempo Real da detecção de Malware.

O sistema Ironport DVS possui rápido escaneamento, ampla cobertura, verifica objetos (binários, true type, mime type) e é desenhado para suportar múltiplas ferramentas de análise.

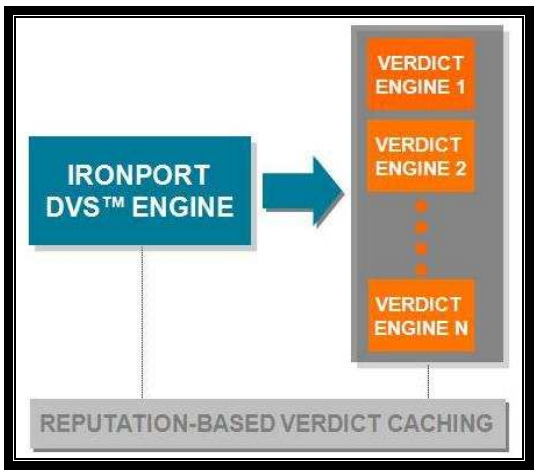


Figura 15 - Esquema de Funcionamento do DVS.

Sua varredura ocorre durante o streaming do arquivo (durante a recepção) e não após a conclusão da sua recepção. Com isto tem-se um ganho escalável de performance.

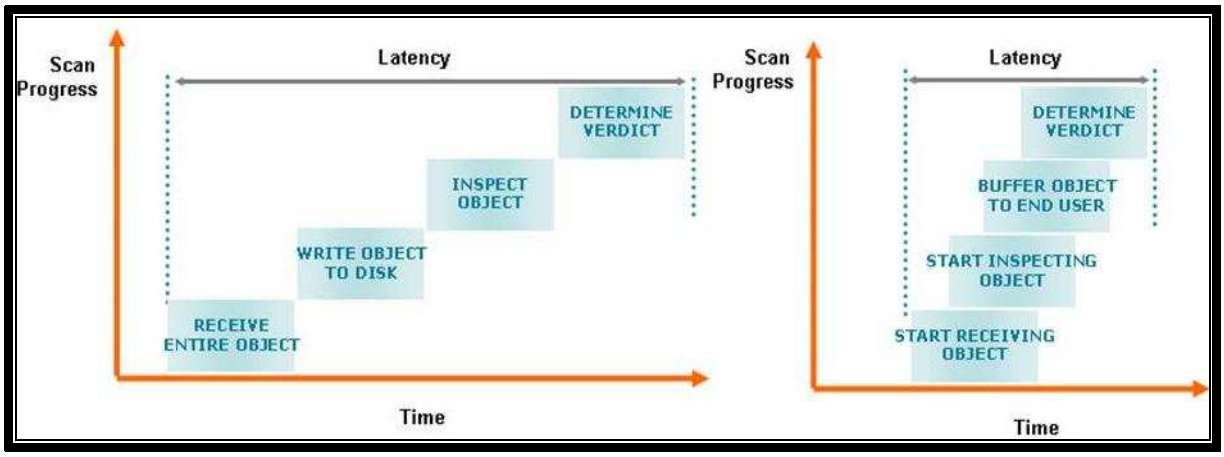


Figura 16 - Comparativo entre a varredura normal e a varredura do streaming de dados.

4.3 MONITORAMENTO DE TRAFEGO CAMADA 4 (L4) IRONPORT

Através do monitoramento de camada 4, procura atividades “phone-home” no qual o aplicativo tenta se comunicar para fora (sites de repositório utilizados pelas aplicações maliciosas) enviando alguma informação confidencial ou baixando novos aplicativos.

É feito uma varredura de alta velocidade na rede em busca de atividades de malware, varrendo as 65.535 portas em altíssima velocidade, capturando malware que tenta “bypassar” a porta 80. É alimentado por uma extensa base de dados anti-malware e possui regras padrão no L4 Monitor.

Possui também a função DNS Discovery para criar novas regras dinamicamente de bloqueio (verifica tentativas de consultar o DNS para sites suspeitos - senderbase), suporta os modos: **somente monitora** ou **monitora e bloqueia** (este funcionando

apenas em topologia em linha), podendo também isentar fontes e/ou destinos e fazer atualizações automáticas.

Desta maneira é possível determinar em quais máquinas está a infecção e combatê-la mais proativamente.

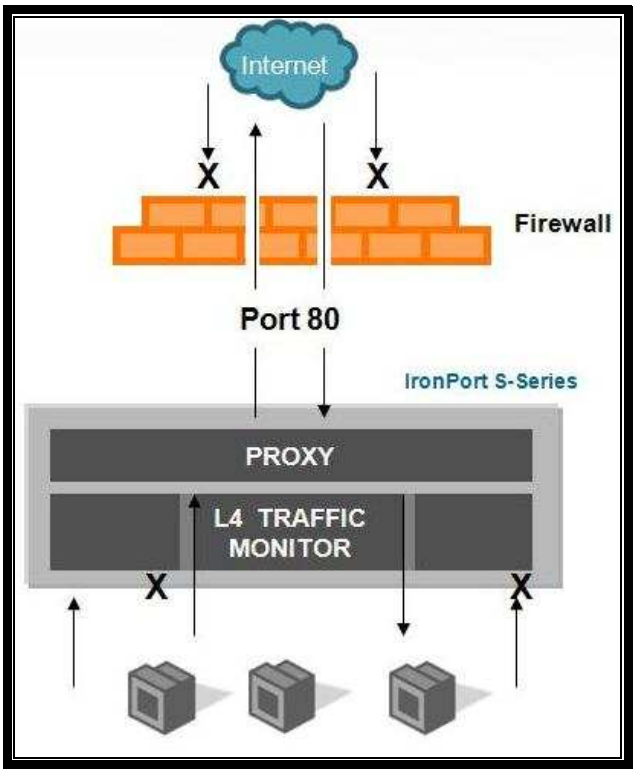


Figura 17 - Esquema de funcionamento do Monitor de Camada 4.

4.4 FILTROS URL IRONPORT

- Gerenciamento flexível de políticas - políticas por usuário e grupo, múltiplas ações, e notificações customizadas;
- Ampla cobertura dos filtros - requisição e resposta, origem e destino e escaneamento completo (por endereço IP, domínio, URLs, expressões regulares, tipo de objeto, tamanho do objeto);
- Ações granulares de acordo com o veredicto;
- Visibilidade - relatórios fáceis de entender, logging extensivo e vários alertas.

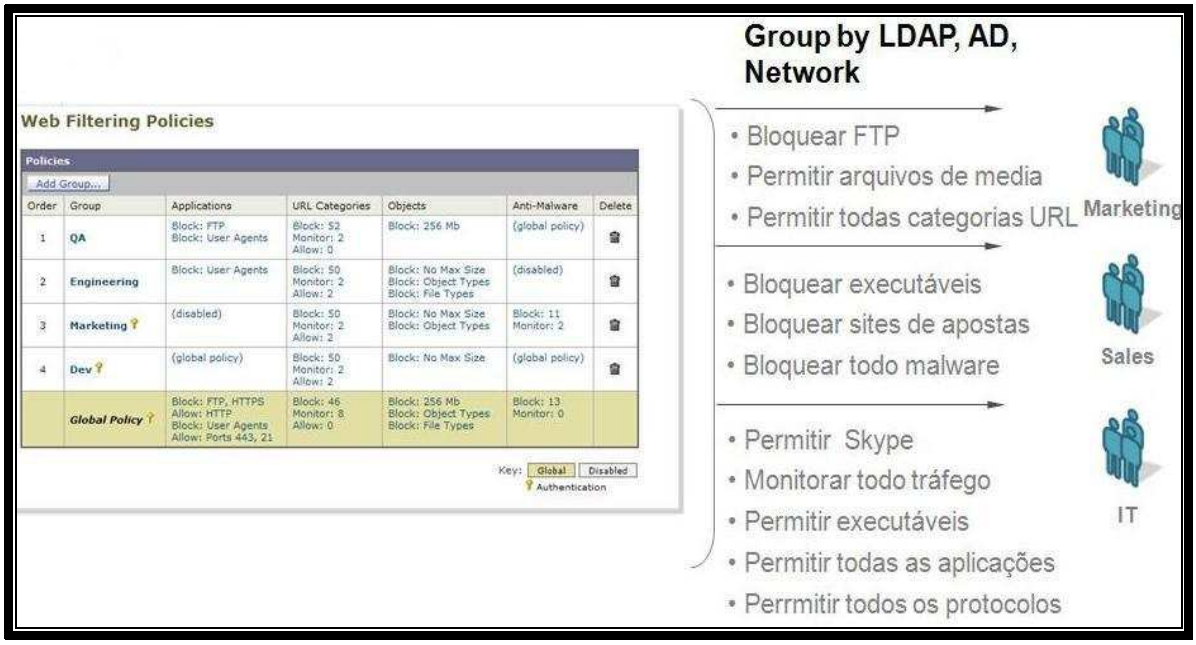


Figura 18 - Possibilidades na utilização do Filtro de URL.

4.5 FILTRO DE CONTEÚDO

É utilizada a base de dados do Surfcontrol que foi recentemente comprado pela Websense.

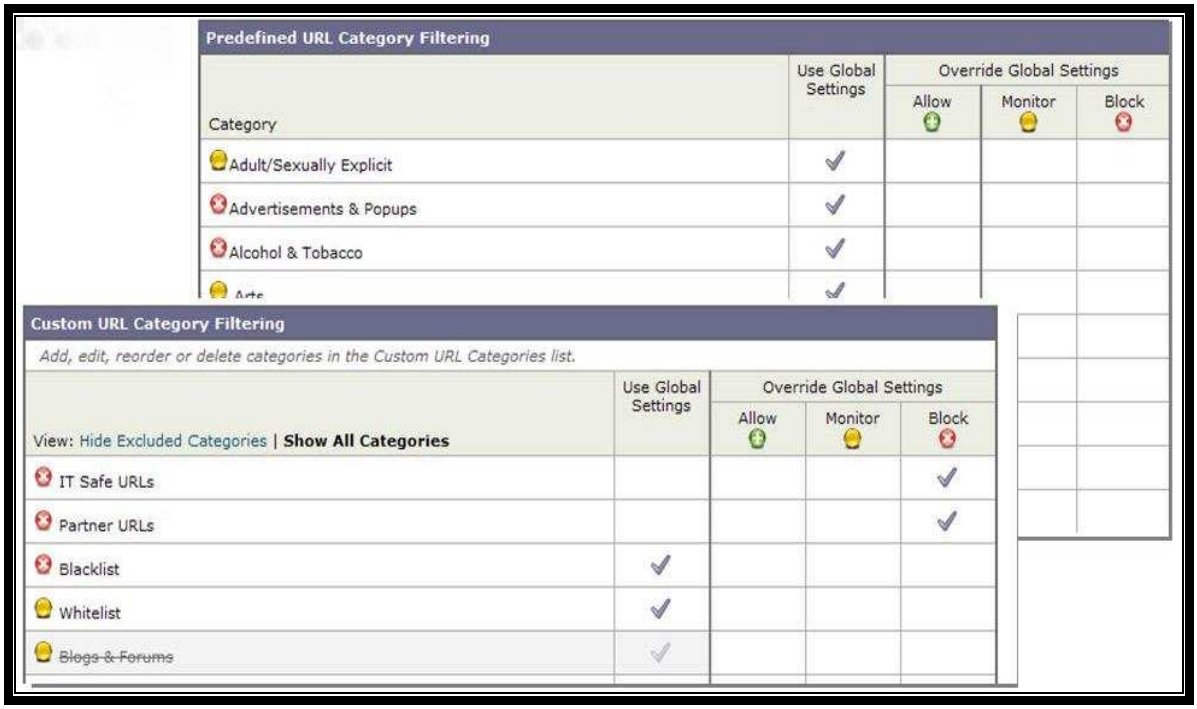


Figura 19 - Tela de configuração do Filtro de URL.

- Ampla base de dados;
- 52 categorias, mais de 21 Milhões de Sites, ~3.5 Bilhões de páginas WEB;
- Cobertura internacional (inclusive Brasil);
- Monitoramento 24 x 7;
- Atualizações regulares e automáticas.

4.6 INTERFACE DE GERENCIAMENTO

Existem dois tipos de interface de gerenciamento: via WEB e via linha de comando (CLI) através do SSH V.2.

Através de usuários e senha (com o uso de chaves privadas ou não), pode-se gerenciar o acesso administrativo ao equipamento.

O equipamento também permite túneis de conectividade criptografada diretamente pelo fornecedor. Isto pode quando solicitado ou quando o auto-suporte estiver habilitado. Em caso de problemas o equipamento avisa ao fornecedor que faz a correção proativamente.

Pode-se configurar inicialmente o equipamento através de um assistente em sete passos, ou podemos importar um arquivo XML de outro equipamento já utilizado, que alem das configurações de rede, vai trazer todas as configurações de políticas.

Pode-se ter diversos níveis de acesso ao equipamento:

- Administrador – Altera qualquer configuração no equipamento;
- Operador – Altera apenas as políticas de acesso dos usuários que utilizam o equipamento;
- Convidado – Acesso apenas de leitura, normalmente utilizado por gerentes e auditores.

4.7 IRONPORT WEB SECURITY MONITOR

Através de uma interface amigável pode-se monitorar todas as atividades dos usuários em tempo real através da guia de monitoramento, além de outras possibilidades como:

Visão do Sistema, *Tendências do Tráfego WEB, Atividade do Site*, *Detalhe do Site*, *Atividade do Usuário*, *Detalhe do Usuário, Detalhe da Categoria, Detalhes do Malware,Tendências de Malware, Monitor de Tráfego L4*, *Reputação WEB.*

Figura 20 – Telas que fazer parte do Security WEB Monitor (em tempo real).

Também no próprio equipamento pode-se gerar relatórios de eventos ocorridos:

- Relatórios de segurança de fácil interpretação;
- Acesso aos dados de relatório em formato CSV;
- Dados disponíveis também via ferramentas de scripting;

Figura 21 - Relatórios de Segurança de eventos já ocorridos.

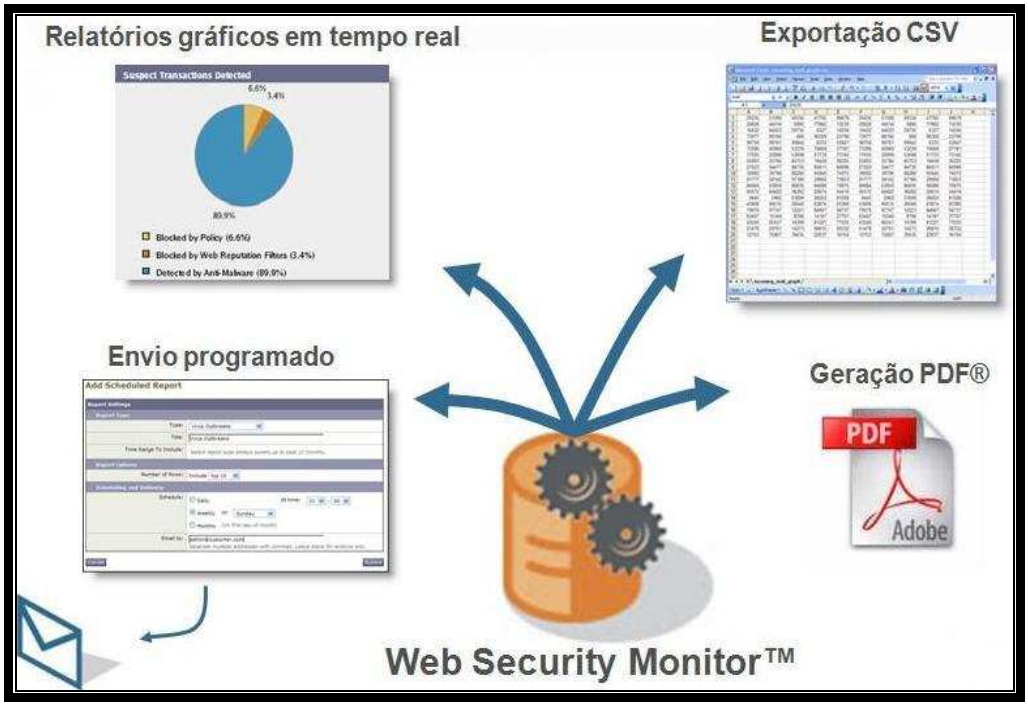


Figura 22 - Ferramenta de Relatórios Versátil.

- Relatórios Cetralizados para análise detalhada do acesso WEB;
- Utilizando software líder – Sawmill;
- Visão detalhada das atividades dos usuários e sites;
- Pode ser totalmente customizado para atender às necessidades do cliente.

4.8 AUTENTICAÇÃO DO USUÁRIO

O equipamento tem diversas opções para tratar da autenticação dos usuários, podendo ser integrado via LDAP com Active Directory - Microsoft (também via NTLM), Edirectory - Novell, OpenLdap e diversos outros tipos de serviços de diretórios, tornando assim o processo de autenticação durante o uso da WEB o mais transparente possível.

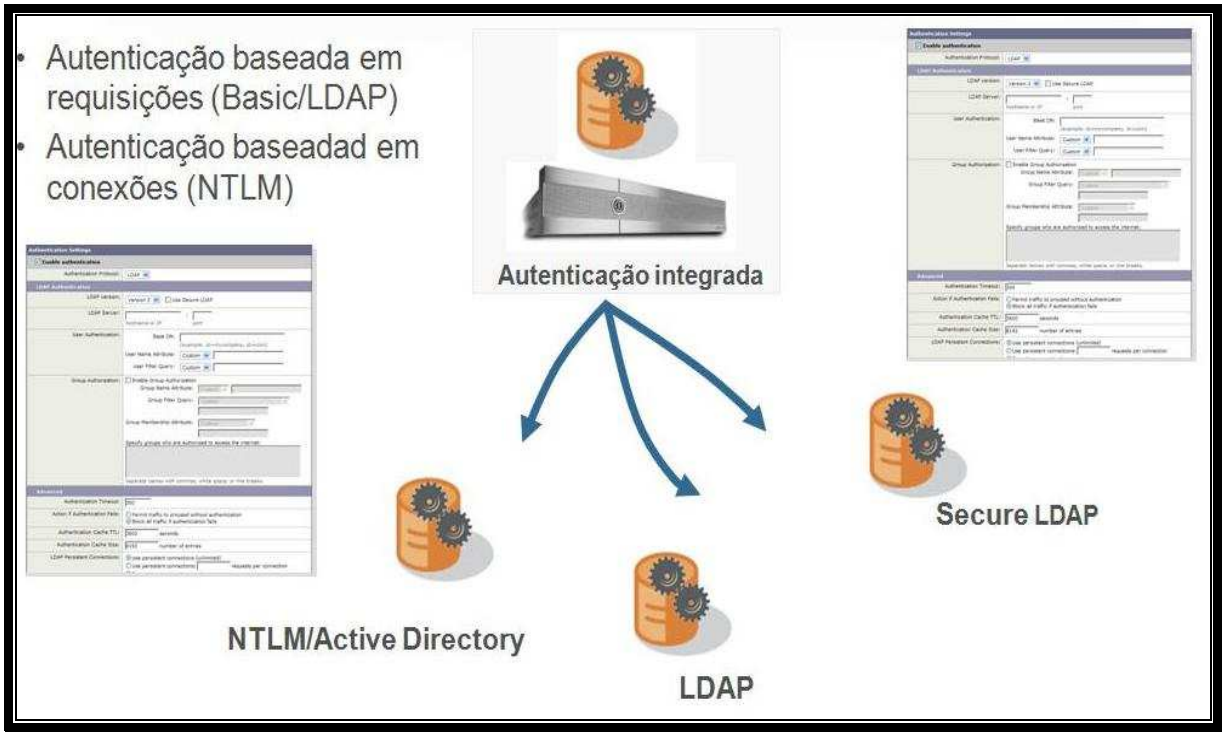


Figura 23 – É possível utilizar diversos tipos de autenticações.

4.9 INTERCEPTAÇÃO SSL (HTTPS)

A função de interceptar conexões SSL é vendida junto com o equipamento (ao contrario do Blue Coat – capítulo seguinte). O conceito desta funcionalidade é ser possível aplicar políticas de segurança mesmo em conexões “tuneladas” (criptografadas), evitando que se impeça de inspecionar o conteúdo em busca de malwares, mesmo que ele seja protegido e classificado como confidencial, para evitar que informações vitais à empresa sejam enviadas para fora da rede corporativa sem autorização do Gestor.

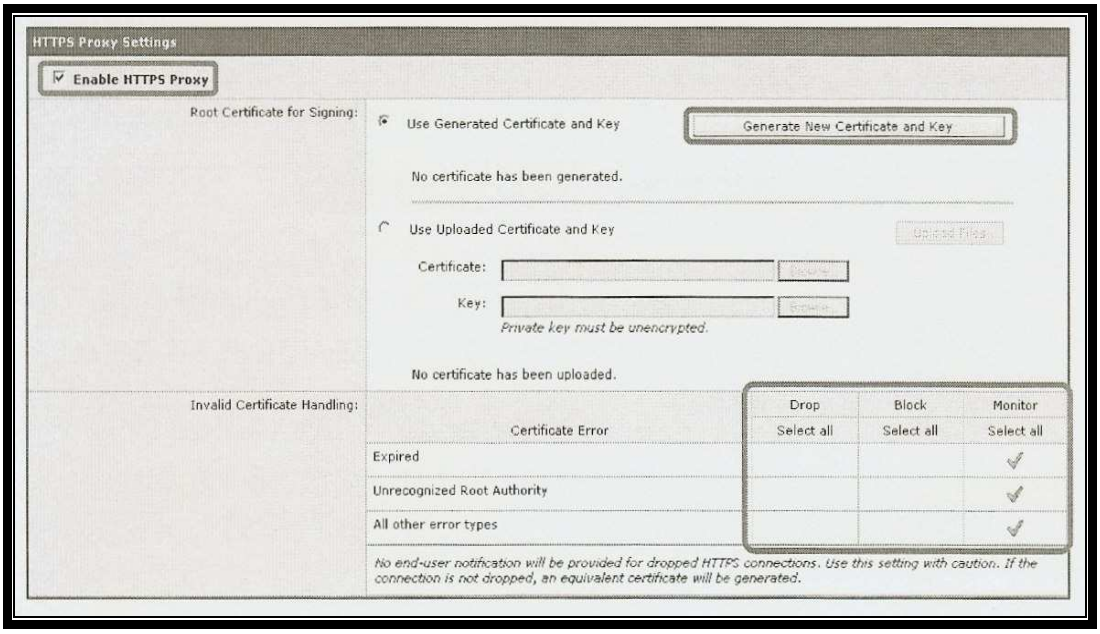


Figura 24 - Painel de Configuração da Interceptação SSL.

Esta decisão de inspecionar ou não o conteúdo da conexão SSL será baseada em políticas definidas no filtro de políticas (mesmo em sites de boa reputação WEB) ou pode ser também baseada na reputação WEB definida pela senderbase. Se o site estiver bem pontuado não haverá inspeção do conteúdo SSL. Para habilitar esta função no equipamento, ela deve ser explicitamente ligada e concordando com os termos legais que o equipamento impõe.

5 SOLUÇÕES BLUE COAT

Figura 25 - Proxy RA 8100

A Blue Coat [5] foi fundada em 1996 com o nome de Cacheflow na função de proxy e cache e em 2002 trocou de nome para Blue Coat, adicionando as funções de controle de políticas e segurança. Em 2006 a empresa elegeu a tecnologia de otimização de wan (Mach5) como foco. Para consolidar em todo este tempo sua posição como líder, a Blue Coat adquiriu as seguintes empresas ao longo de sua historia:

- 1996 - Scalable Data Systems
- 2000 - Springbank Networks
- 2000 - Entera
- 2003 - Ositis Software
- 2004 - Cerberian
- 2006 - Permeo Technologies
- 2006 - NetApp's NetCache product line
- 2008 - Packeteer

Os equipamentos Blue Coat utilizam um micro kernel chamado SGOS, que derivou do projeto *Thoth* da Universidade de Waterloo [8], considerado o primeiro kernel de tempo real, e um dos seus descendentes é o QNX que é o sistema pai do SGOS (da Blue Coat). O SGOS possui as certificações NIAP Evaluation Assurance Level 2, FIPS 140-2 e ICSA.

Existem diversos equipamentos e softwares que compõem a solução de segurança da Blue Coat: ProxySG (recomenda-se 2 equipamentos por questões de redundância) que é propriamente o Proxy; Proxy AV, que é um equipamento de escaneamento de malware; Blue Coat Reporter - software (Windows ou Linux), instalado em servidor dedicado, é o sistema de relatórios que utiliza os logs gerados pelo ProxySG para montar relatórios executivos; e o BCAAA, que é um software que realiza a autenticação dos usuários da rede local que utilizam o Proxy SG no ambiente Active Directory da Rede Windows da empresa.

Figura 26 - Equipamentos e Software Diversos montam a solução da Blue Coat.

O Blue Coat Proxy SG além de WEB (HTTP, HTTPS e FTP) faz controle de muitos outros protocolos entre eles: CIFS, MAPI, Telnet, SOCKS, P2P, Microsoft Media Services, RTSP, QuickTime, AOL IM, Yahoo IM, MSN Messenger, e TCP-Tunnel.

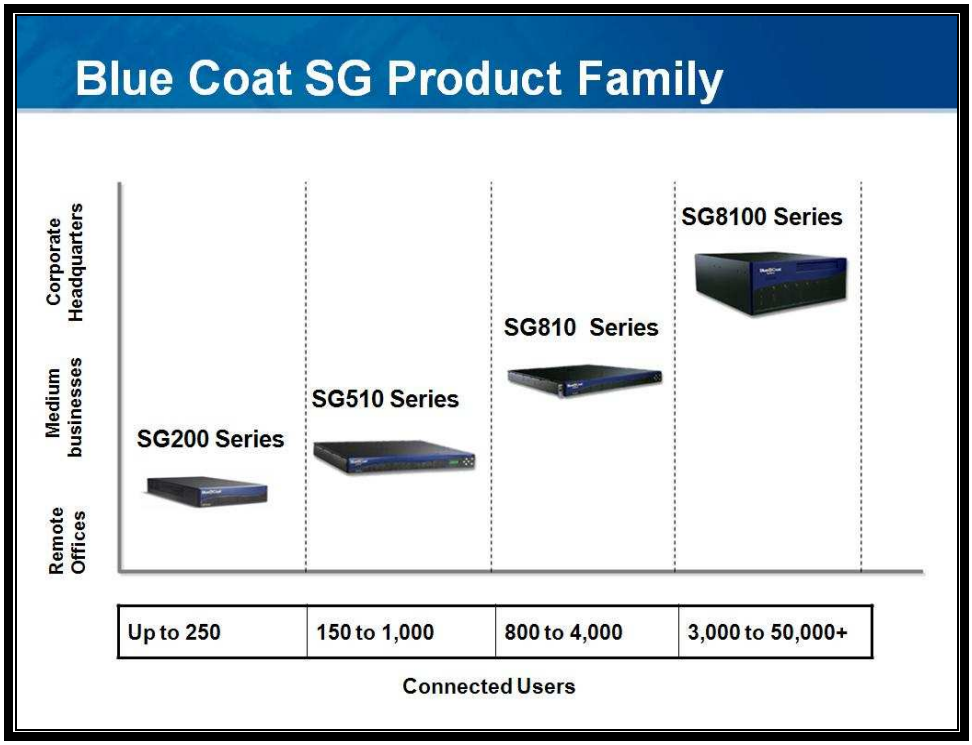


Figura 27 - Equipamentos para diversas demandas.

O Proxy SG armazena os objetos em disco de forma que leve em consideração o alto desempenho e a escalabilidade. Isto determina quão rápido este objeto será recuperado quando solicitado pelo cliente de rede local e quão rápido este objeto será armazenado no disco (também da velocidade que um cliente poderá acessar este objeto).

O sistema de armazenamento de objetos não é um sistema de arquivos convencional, é um cache de objetos. Não existe diretório neste sistema de armazenamento, o acesso ao objeto é feito a partir de um mapeamento de hash na memória RAM, garantindo que qualquer objeto será obtido em uma simples leitura ao disco.

Sistemas de arquivos convencionais rodam com baixo desempenho quando estão ao fim da sua capacidade de armazenamento, enquanto o sistema de armazenamento de objetos (cache de objetos) roda com mais desempenho quanto mais perto do fim de sua capacidade.

Fica armazenado no disco objetos que são referenciados por uma parte do nome url e o acesso é automaticamente balanceado entre os discos (SCSI) disponíveis. O equipamento roda normalmente com o disco cheio em sua capacidade com os objetos. Objetos mais antigos são continuamente removidos para abrir espaço para novos objetos.

Quando um disco falha, os objetos são automaticamente mapeados para os discos remanescentes. Novos discos podem ser adicionados, mesmo com o equipamento ligado, para aumentar sua capacidade de armazenamento. Não é utilizado nenhum tipo de RAID, pois em nada contribui para o aumento da velocidade para o WEB cache e ainda diminui a capacidade de armazenamento dos objetos.

Quando é feita uma requisição convencional de um site, o Proxy vai baixando objetos um a um do site e entregando ao solicitante.

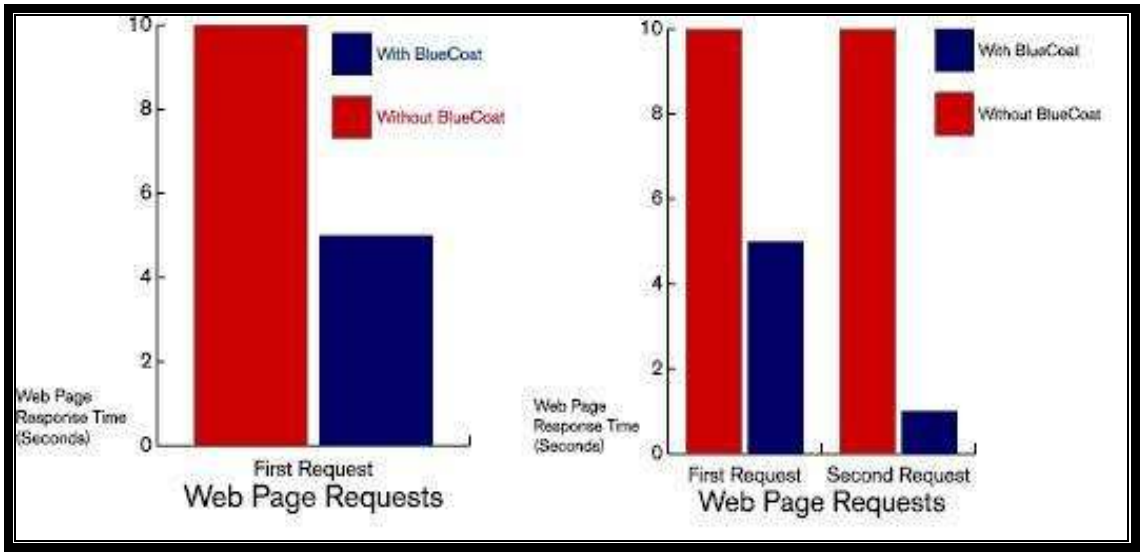


Figura 28 - Demonstrativo da eficiência dos algoritmos de otimização do Blue Coat.

O Blue Coat utiliza um algoritmo chamado “Object Pipelining” que abre várias conexões simultâneas para aquela mesma url, trazendo vários objetos daquele site ao mesmo tempo, acelerando em muito a velocidade a sites que estejam sendo acessados pela primeira vez.

Outro algoritmo que contribui para a velocidade da requisição em segunda solicitação ao Proxy é o “Adaptive Refresh”.

O Proxy SG verifica a popularidade das solicitações do site, verifica que partes deste site são mais dinâmicas e quais são mais estáticas. Com essa informação o Proxy SG atualiza periodicamente os objetos que mudam mais freqüentemente, e desta maneira, reduz o consumo de banda.

5.1 TOPOLOGIA DE IMPLANTAÇÃO

O Proxy SG pode ser implantado de duas formas diferentes:

- Encaminhamento ou Foward (Explicito ou Transparente)
- Reverso

5.1.1 Explícito

É necessário definir explicitamente no navegador do cliente de rede local onde o navegador deve solicitar as urls, sendo os demais protocolos não tratados pelo navegador encaminhados as default gateway (normalmente um roteador ou firewall).

A implementação é simples no servidor, porém nos clientes poderá ser feito através de configurações individuais ou uso de Group Policy em ambiente Active Directory Windows Server.

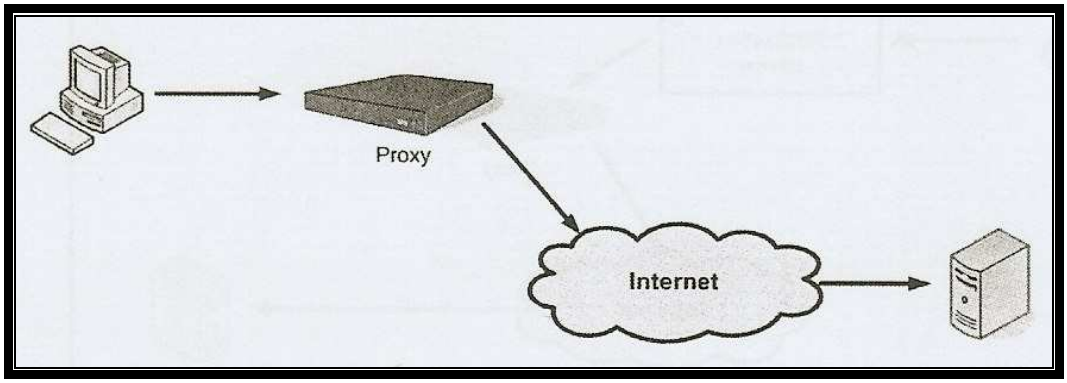


Figura 29 - Topologia de Proxy Explicito.

5.1.2 Transparente

Não se faz necessário a configuração do navegador, pois todos os protocolos ou alguns (somente os que interessam ao navegador) serão redirecionados ao Proxy, seja redirecionados fisicamente (em modo bridge – in line) ou redirecionado logicamente (através de switch camada 4, roteador utilizando wccp, redirecionando através de firewall ou sendo apontado como default gateway).

Se o Proxy SG não estiver explicitamente ativado para tratar (interceptar) determinado protocolo, ele o deixará passar livremente através do Proxy SG (lembrando que o Proxy SG tem capacidade para interceptar somente alguns protocolos).

Configuração é mais complexa no servidor, porém nenhuma configuração é necessária para atender os navegadores dos clientes de rede local.

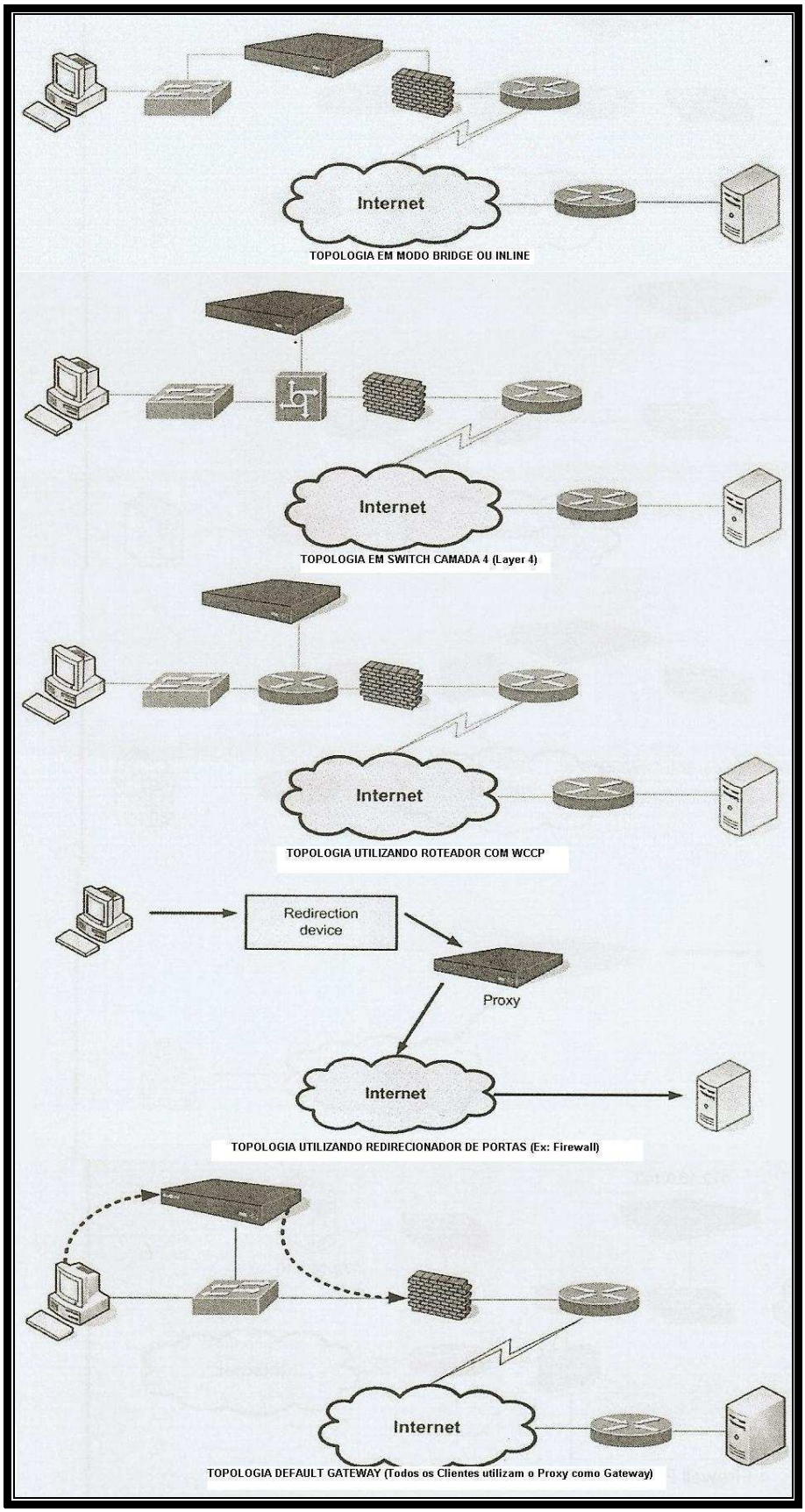


Figura 30 - Topologias de Proxy Transparentes.

5.1.3 Reverso

Com o Proxy Reverso é possível entregar conteúdo de um ou mais servidores WEB. Todo tráfego é direcionado ao servidores de fim de linha (servidores WEB) que por sua vez são redirecionados para o Proxy SG. Algumas motivações para instalar um servidor Proxy reverso: proteger e assegurar os servidores por trás do mesmo; distribuir a carga através deles; fazer cache do conteúdo estático; compressão do conteúdo; e integração total de conexões SSL via Proxy SG.

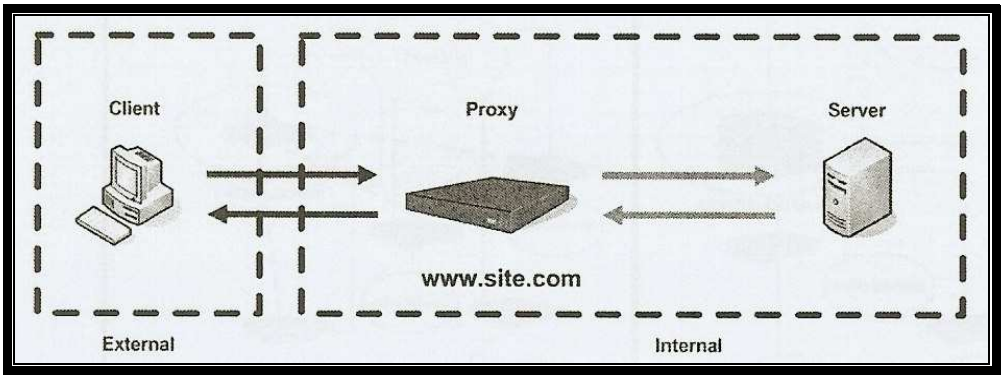


Figura 31 - Topologia de Proxy Reverso.

5.2 PROXY AV

No conjunto de produtos Blue Coat temos o Proxy AV que é um equipamento dedicado a combater vírus e spywares. Ele se comunica com o Proxy SG através do protocolo ICAP, possuindo os seguintes fabricantes: Kaspersky Lab, McAfee, Sophos, Ahn Lab e Panda Software.

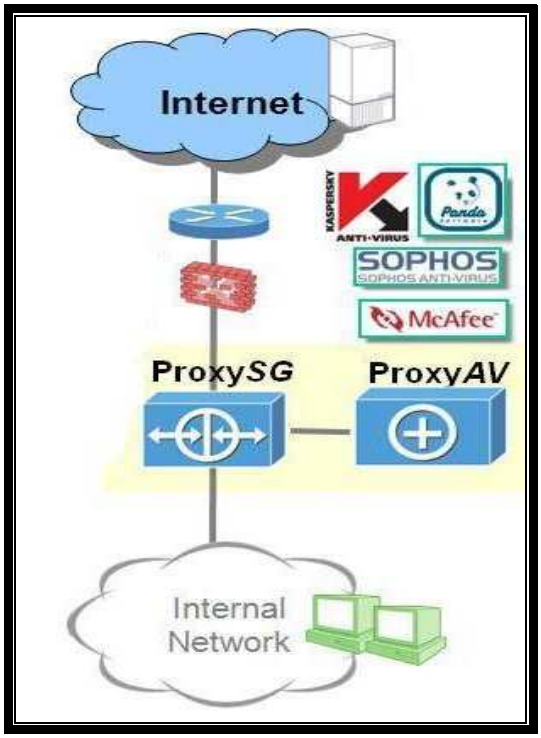


Figura 32 - Engine de Fabricantes de Antivírus suportados pelo Proxy AV.

5.3 AUTENTICAÇÃO DO USUÁRIO

Proxy SG da Blue Coat oferece integração com várias tecnologias de autenticação:

- IWA (Internet Windows Authentication), LDAP, RADIUS, Local, Certificate, Sequences, NetegritySiteMinder, Oracle COREid, Policy Substitution e etc.

O método de autenticação mais utilizado é **Integrated Windows Authentication** (IWA), um termo usado pela Microsoft que se refere a uma combinação de protocolos de autenticação como SPNEGO, Kerberos, e NTLMSSP

Figura 33 - Tipos de Autenticações Suportados.

- IWA o é mais usado como solução de autenticação com domínios Windows.
- BCAAA (Blue Coat Systems Authentication and Authorization Agent) é instalado em uma máquina membro do domínio ou floresta. Usa endereço IP fixo, porta 16101 aberta entre o agente e o Proxy SG para ocorrer a sincronização.
    - Obs. IMPORTANTE: versão do BCAAA deve ser compatível com o SGOS do equipamento.
- Uma vez que o usuário esteja autenticado, pode-se controlar de uma maneira granular seu tipo de acesso na rede através de desenvolvimento de Políticas.

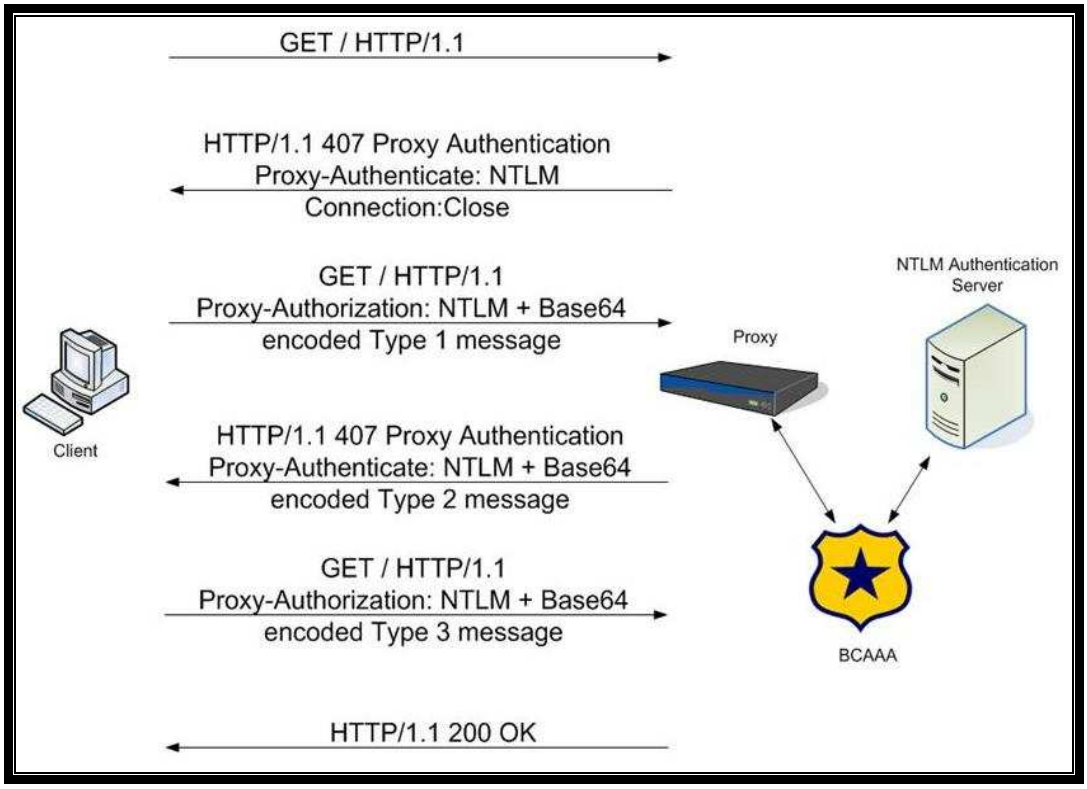


Figura 34 - Funcionamento da Autenticação NTLM (Windows).

5.4 INTERFACE DE GERENCIAMENTO

O Proxy SG pode ser administrado através da sua própria interface WEB (baseada em Java); por linha de comando (CLI – Command Line Interface) conectando-se por SSH na porta 22; ou pelo Blue Coat Director (Gerenciador de vários equipamentos Blue Coat através da porta SSH, porém fornecendo interface gráfica em Java centralizadora). Na figura 35, algumas das opções de configuração, basicamente dividido em Configuração, Manutenção e Estatísticas.

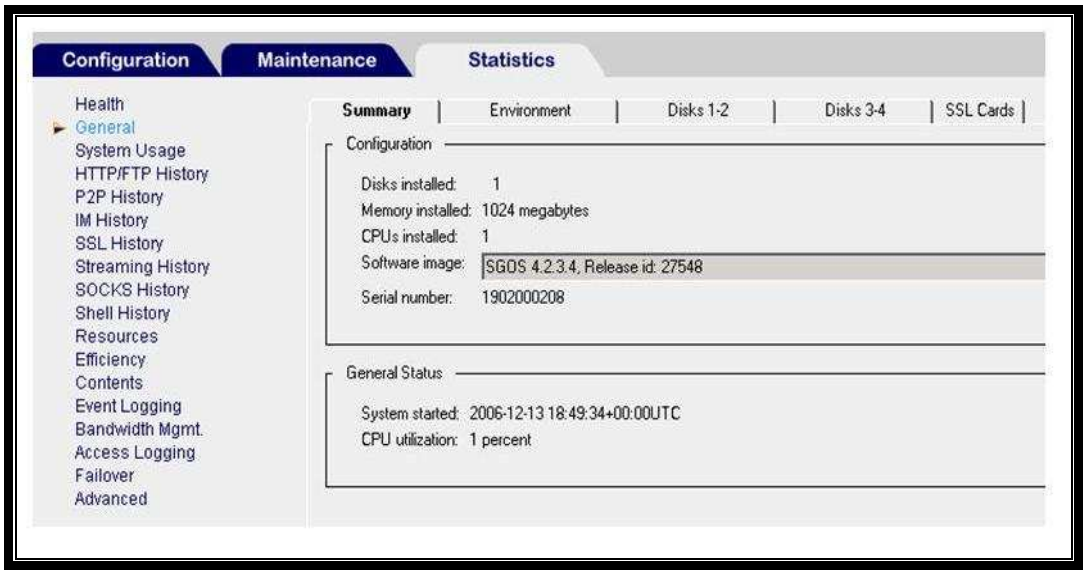


Figura 35 - Tela Principal quando entra na Interface WEB.

Em um único equipamento pode-se ter varias versões de sistema operacional (SGOS) instaladas, porém somente pode ser utilizado uma por vez. Na figura 36, podemos ver em detalhes o sistema de gerenciamento de SGOS e de Upgrade de SGOS.

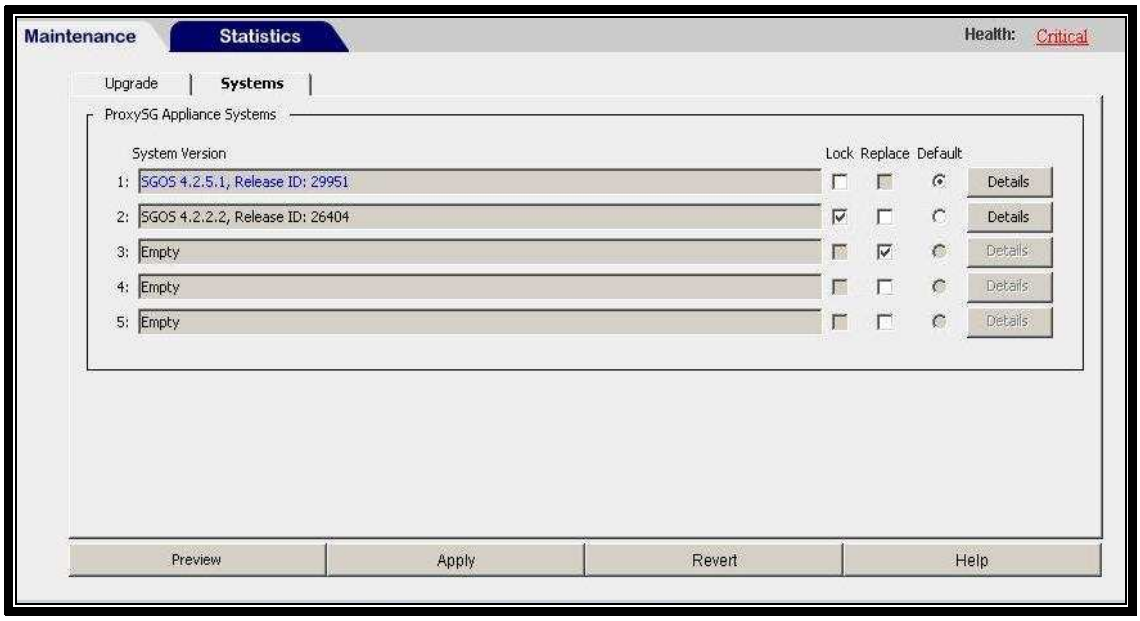


Figura 36 - Gerenciamento de Versões do Sistema Operacionais do Equipamento.

O Proxy SG pode “tratar” diversos protocolos de aplicação (dependendo da forma como foi implementado na topologia da rede). Ele pode ser configurado para interceptar determinados tipos de protocolos ou para ignorá-los e deixar que passem sem qualquer interferência.

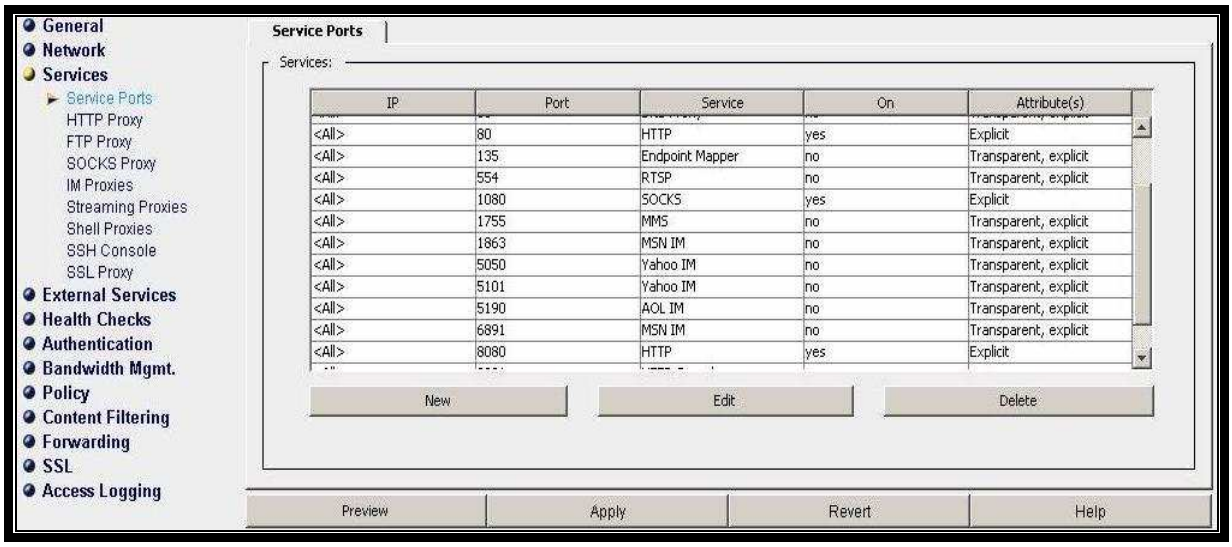


Figura 37 - Administração de protocolos a serem interceptados pelo Proxy SG.

5.5 VISUAL POLICY MANAGER (VPM)

- VPM é sua ferramenta padrão para fazer alterações na política de autorização dos clientes;
- VPM usa o conceito de camada;
- Cada camada criada pode possuir centenas de regras;
- Todas as camadas criadas se baseiam no conceito de DENY ou ALLOW;
- Para clientes com muita restrição aplica-se o conceito DENY tudo, e liberando algumas coisas;
- Para clientes com pouca restrição aplica-se o conceito ALLOW tudo, bloqueando algumas coisas (mais popular e menos impactante);

- Regras são varridas pelo Proxy de cima para baixo em uma camada específica, e da esquerda para a direita entre as camadas.

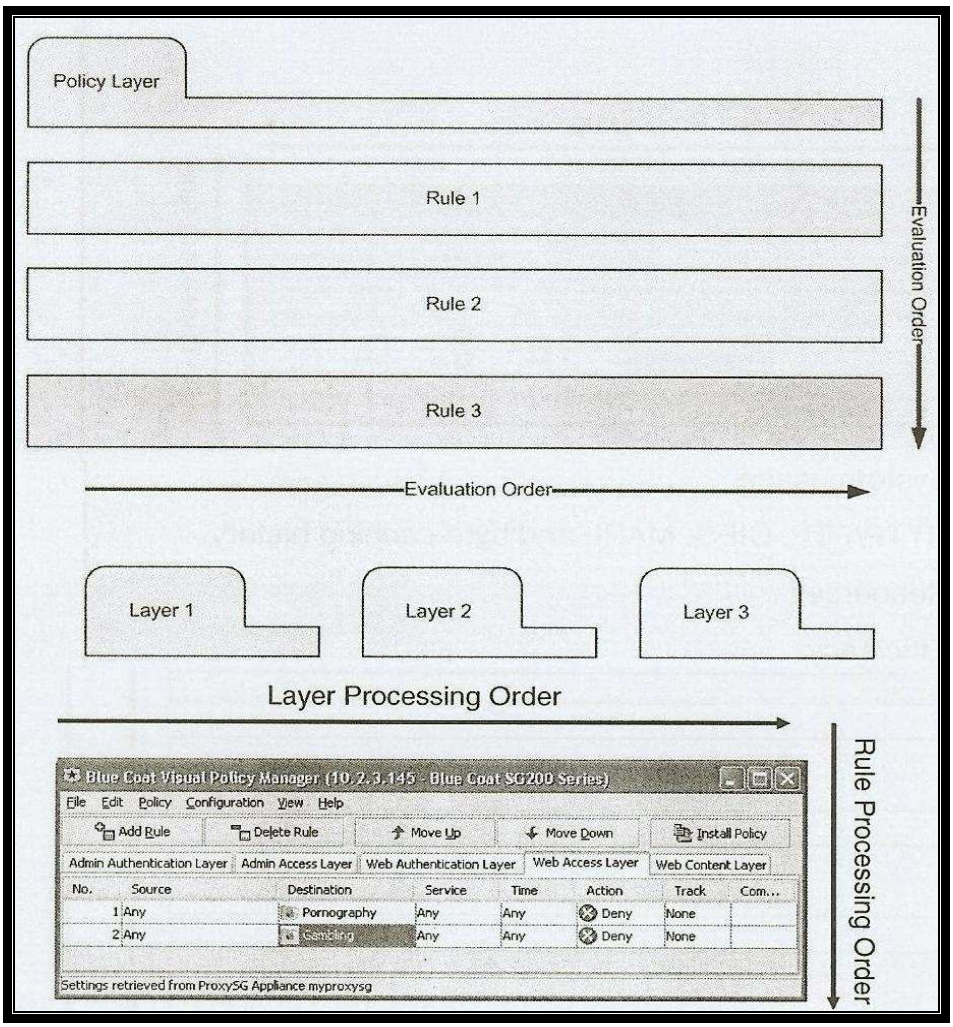


Figura 38 – Funcionamento de como as regras da política é processada.

O VPM possui camadas pré-definidas que podem ser utilizados uma ou mais vezes. Por exemplo, pode-se ter duas camadas WEB access e trocar seu nome na guia de identificação para melhor identificá-la. Algumas destas camadas pré-definidas são:

- Administration Authentication – Determina como os administradores devem se autenticar ao acessarem o Proxy SG;
- Administration Access – Determina quem pode acessar o Proxy SG para realizar tarefas administrativas;

- DNS Access – Determina como o Proxy SG deverá tratar requisições DNS;
- SOCKS Authentication – Determina que método de autenticação deverá utilizar para acessar o Proxy SG utilizando SOCKS;
- SSL Intercept – Determina quando poderá trafegar via túnel SSL ou interceptar o SSL;
- SSL Access – Determina quando determinado destino terá o acesso SSL proibido ou permitido;
- WEB Authentication – Determina como e se um usuário deve se autenticar quando acessar um site WEB via Proxy SG;
- WEB Access – Determina que recursos vão ser proibidos ou permitidos aos clientes acessando um site WEB via Proxy SG;

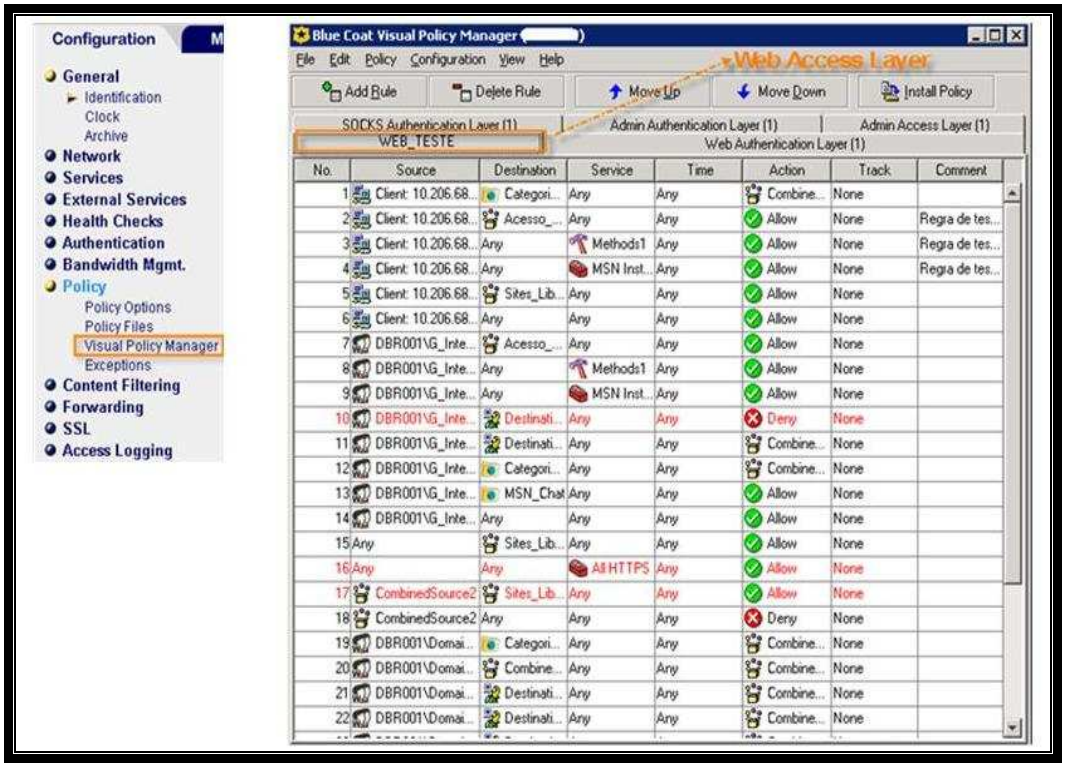


Figura 39 - VPM sendo utilizado em ambiente de produção.

- WEB Content – Determina se será feito cache ou não de um destino solicitado e se terá seu trafego redirecionado para o Proxy AV para inspeção de Malware;

- Fowarding – Determina o redirecionamento de hosts e métodos (POST e GET).

5.6 FILTRO DE CONTEÚDO

O Filtro de conteúdo utilizado no Proxy SG pode se localizar dentro do equipamento (diversas marcas, inclusive da própria Blue Coat) ou fora do equipamento (somente o WEBsense).

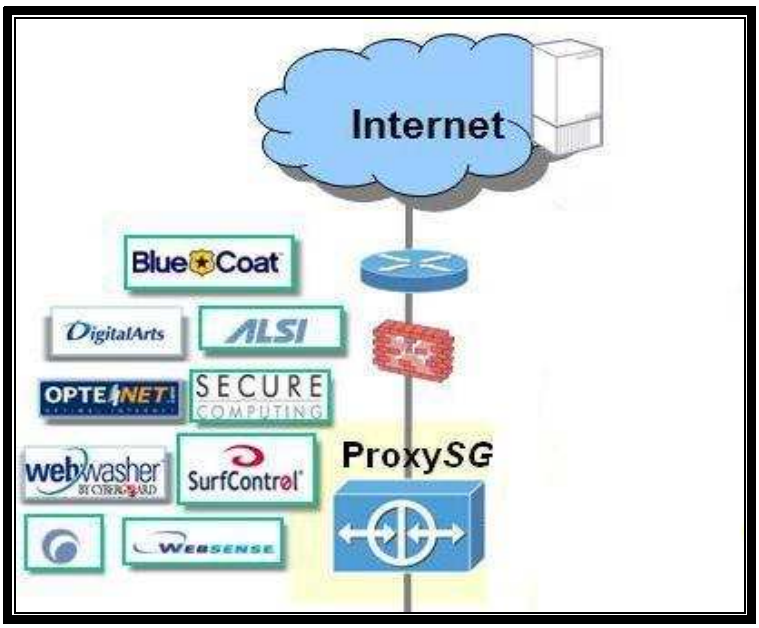


Figura 40 - Marcas de Filtros de Conteúdo compatíveis com o Proxy SG.

Por razões de desempenho é recomendado que se utilize o filtro de conteúdo dentro do próprio equipamento. O filtro de conteúdo é uma base de dados contendo urls e sua classificação por categorias baseadas no conteúdo do site.

O filtro de conteúdo por si não bloqueia nada, o bloqueio é realizado através das regras que são implementadas preferencialmente via VPM.

Desta maneira ao invés de bloquear url por url de sites pornográficos, por exemplo, basta uma única regra no VPM bloqueando a categoria porn. Uma url poderá pertencer a uma ou mais categorias.

Além da base de filtro de conteúdo comprada, é possível criar uma base de filtro de conteúdo local que será alimentada pelo administrador do Proxy SG.

Após ativar o número de série do filtro de conteúdo comprado, deve-se baixar a base de dados atualizada pelo próprio equipamento e agendar seu download incremental diário para que a mesma se mantenha atualizada.

Pode-se cobrir 80% das regras apenas utilizando regras de categorias através do filtro de conteúdo.

5.6.1 Blue Coat WEB Filter (BCWF)

O BCWF utiliza uma abordagem hibrida como solução de filtro de conteúdo. Fornece uma lista estática que é atualizada (cobre 94% das requisições solicitadas) e diariamente é feito o download para o equipamento.

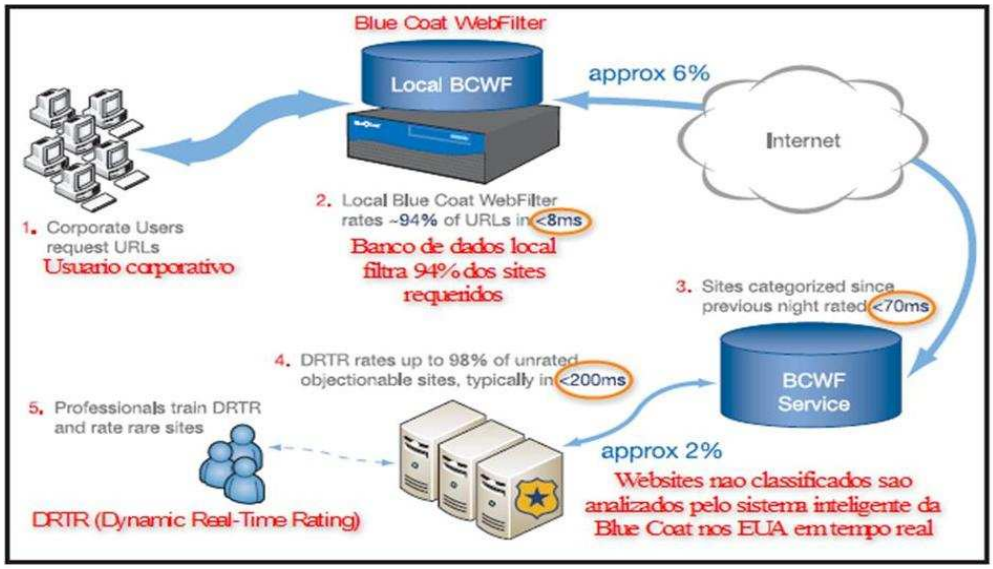


Figura 41 – Funcionamento do Sistema de Classificação do BCWF.

Também oferece o Remote Dynamic Categorization enviando as requisições para o Dynamic Real-Time Rating (DRTR) em caso da url requisitada não estar ainda categorizada na base de dados do BCWF e que foi feito o download até aquele

momento, sendo categorizada em tempo real (categorizando 98% dos sites encaminhados ao DRTR).

O BCWF possui aproximadamente 70 categorias em mais de 50 idiomas (Português do Brasil , inclusive), e mais de 100 Milhões de urls cadastradas.

Uma pequena porção de urls não categorizadas pelo sistema de DRTR automatizado é transferida para categorização humana em diversos pontos do planeta. Este mesmo grupo também analisa os pedidos de reclassificação de urls (em caso de classificação errônea ou mudança de categoria de uma url), que chegam através do site da Blue Coat.

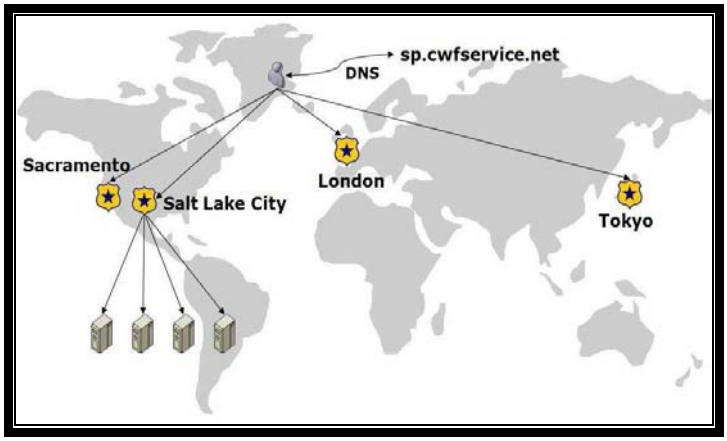


Figura 42 – Localização Geográfica dos agente de categorização humana.

Top Languages			
Category	Probability	Threshold	P/R
english	1.00000	0.50000	0.97 / 0.99
slovenian	0.00000	0.50000	1.00 / 0.98
italian	0.00000	0.50000	1.00 / 1.00
chinese	0.00000	0.50000	1.00 / 0.97
Top Categories			
Category	Probability	Threshold	P/R
Sports/Recreation/Hobbies	1.00000	0.57908	0.80 / 0.60
News/Media	0.00000	1.00000	0.83 / 0.73
Education	0.00000	0.98417	0.80 / 0.78
Miscellaneous	0.00000	NEVER	1.00 / 0.23

Figura 43 - Tabela com resultados de Categorizações e localizações.

Todo o processo de localização geográfica do conteúdo de determinado site é automatizado utilizando algoritmos especializados (baseados em inteligência artificial) com alta taxa de acerto. Pode-se definir que filtros de conteúdo serão utilizados, podendo haver mais de um ativo. Também pode-se consultar no próprio equipamento como (em que categoria) ele reconhece uma determinada URL.

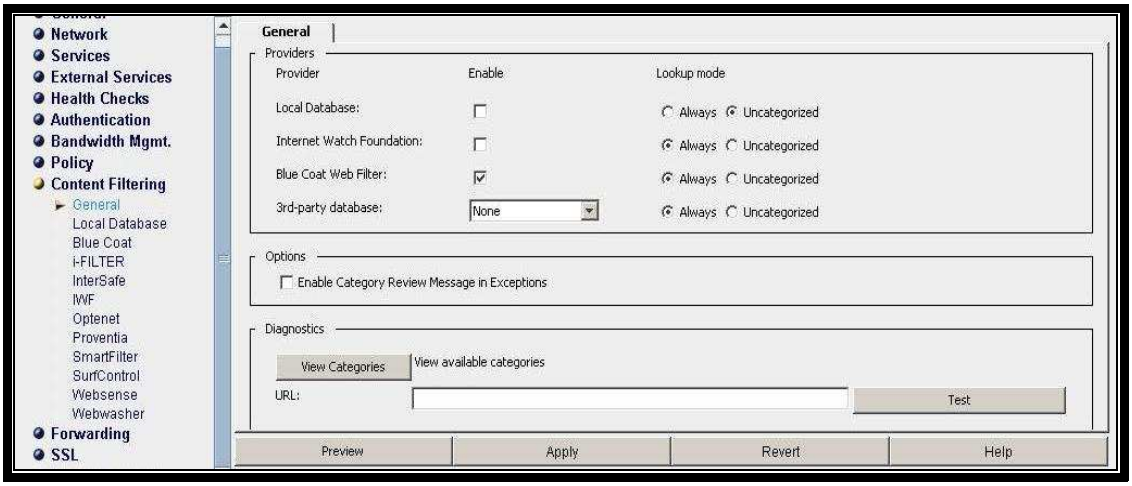


Figura 44 - Configuração Geral do Filtro de Conteúdo.

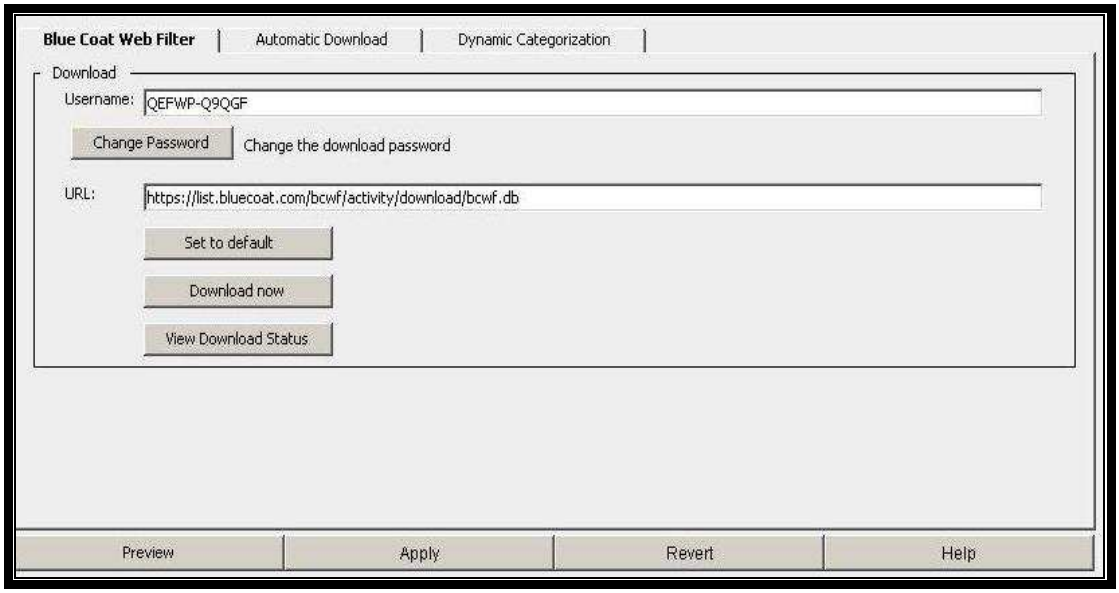


Figura 45 - Configuração do Blue Coat WEB Filter.

Em relação ao Filtro de Conteúdo da Blue Coat pode-se iniciar o Download da Base de Dados imediatamente ou podemos agendá-lo através de um procedimento

bastante flexível. Nesta também é definido como o equipamento vai se comportar em caso de não localizar a url na base de dados local do BCWF. Nesse caso o acesso pode ser negado ou pode ser feito o encaminhamento ao DRTR, em caso de demora na resposta do DRTR, qual o comportamento a ser utilizado.

5.7 INTERCEPTAÇÃO DE SSL (HTTPS)

A função de proxy SSL é vendida como uma licença em separado da licença do Proxy SG. O conceito desta funcionalidade é que seja possível aplicar políticas de segurança mesmo em conexões “tuneladas” (criptografadas), evitando que seja impedido de inspecionar seu conteúdo. Obviamente, por motivos éticos, deve-se colocar as categorias Finacial Services e Investments fora da interceptação do Proxy SSL. Tudo vai ficar registrado em Log que depois poderá ser analisado no Blue Coat Repórter.

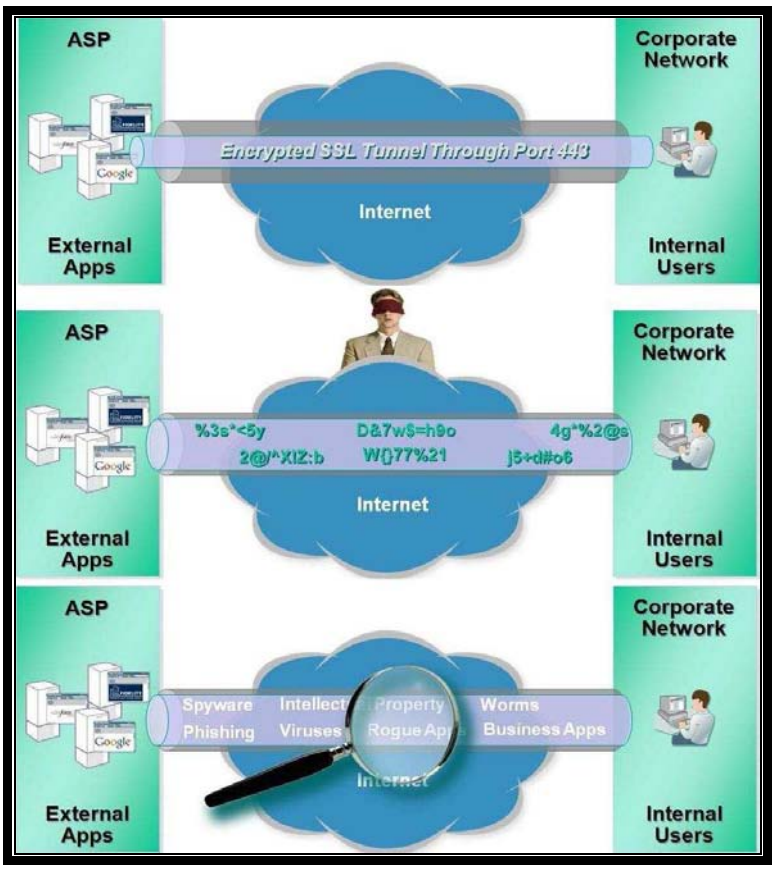


Figura 46 - Esquema demonstrando os perigos de não se inspecionar o SSL.

O proxy SSL funciona da seguinte forma:

1 – O Cliente envia um SSL Client Hello para o Proxy SG;

2 – O Proxy SG envia um Client Hello para o Servidor Destino;

3 – O Servidor destino envia o Server Certificate para o Proxy SG;

4 – O Proxy SG envia para o cliente o seu próprio certificado.

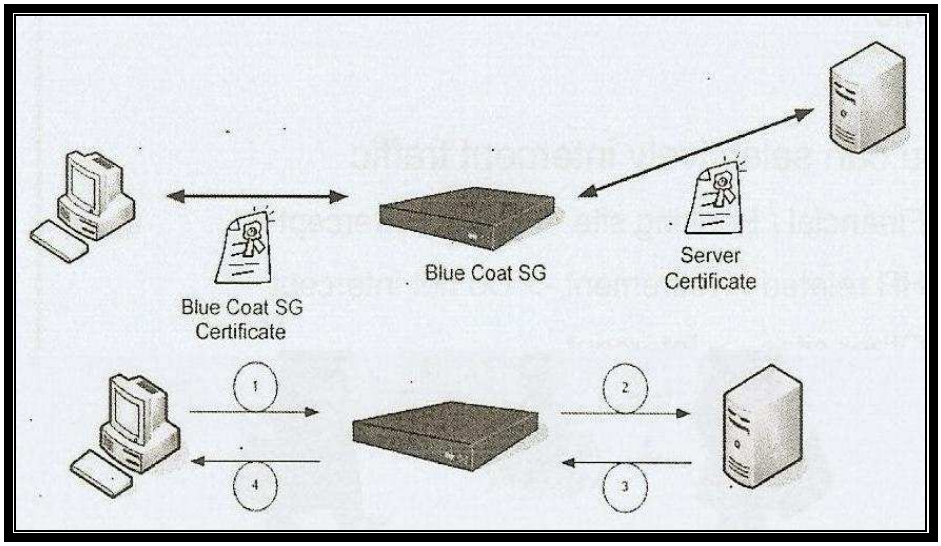


Figura 47 - Esquema demonstrativo sobre a troca de certificados na conexão HTTPS

Deve-se deixar habilitado a interceptação nas configurações gerais do Proxy SSL e dizer explicitamente no VPM (nas camadas SSL Intercept e SSL Access) o que deve e o que não deve ser interceptado.

5.8 MACH5 (MULTIPROTOCOL ACCELERATED CACHING HIERARCHY)

O MACH5 é um conjunto de tecnologias de aceleração pensado para tornar mais veloz as aplicações vitais aos negócios das empresas. Podem ser aplicações WEB e aplicações WEB seguras (SSL), arquivos, Microsoft Exchange (MAPI), streaming de vídeo ao vivo ou pré-gravado e aplicações baseada em TCP/IP.

Por integrar-se ao Proxy SG, o MACH5 viabiliza que se gerencie as interações entre os usuários e aplicações via WAN, seja para proibir aplicações indevidas, restringir o

acesso a aplicações de menor prioridade ou acelerar as que são vitais para a empresa, mesmo quando utilizam criptografia SSL.

Esta é a tecnologia chave para a Blue Coat e seu esforço em melhorar cada vez mais a tecnologia de otimização de aplicações em links WAN. A Blue Coat comprou a Packeteer em maio de 2008, empresa líder em otimização de aplicações em links WAN.

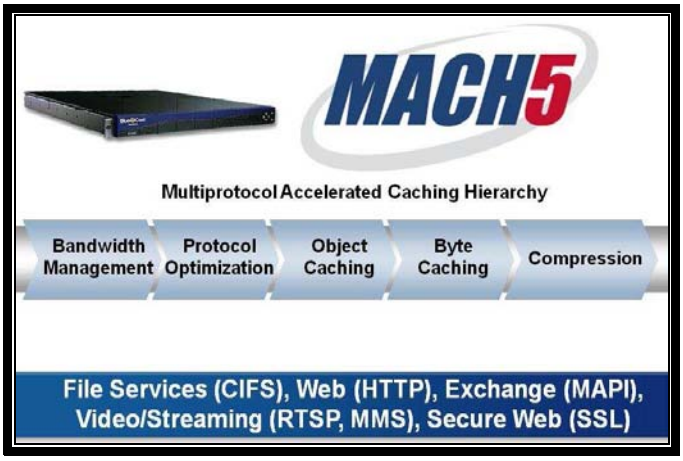


Figura 48 - Os 5 motivos do nome MACH5.

Figura 49 - Descrição das Etapas do Mach5.

5.8.1 Gerenciamento de Banda

Realiza priorização de tráfego para determinadas aplicações ou usuários e reserva banda de transmissão, impedindo que aplicações menos importantes roubem a banda destinada à aplicação principal.

Figura 50 - Exemplo de Utilização do Controle de Banda.

5.8.2 Otimização de Protocolos

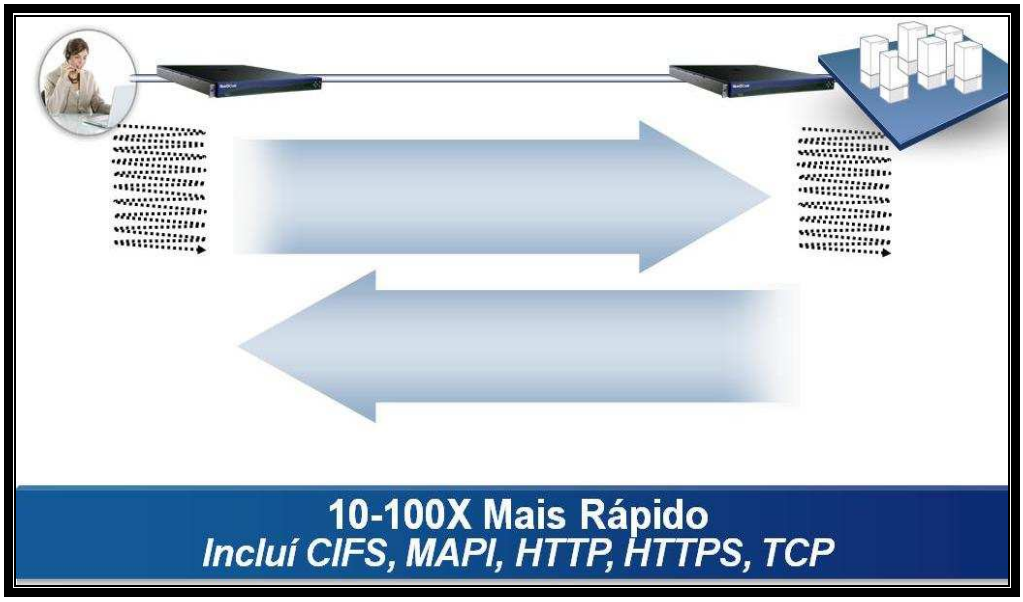


Figura 51 - Otimização de Protocolos.

São feitos alguns “consertos” em protocolos que são ineficientes sobre o link WAN, incluindo Common Internet File System (CIFS), Messaging Application Programming Interface (MAPI), HTTP, Transmission Control Protocol (TCP) and HTTPS, tornando-os mais eficientes. Esta otimização inclui enviar os dados em paralelo quando em seu modo original eles são enviados serialmente.

5.8.3 Cache de Objetos

Armazena uma cópia de objetos (não se restringe apenas a objetos WEB) mais comumente utilizados para que não seja necessário retransmiti-los mais de uma vez atualizando o objeto se o mesmo for modificado, mas esta atualização ocorre apenas quando ele for enviado através da WAN.

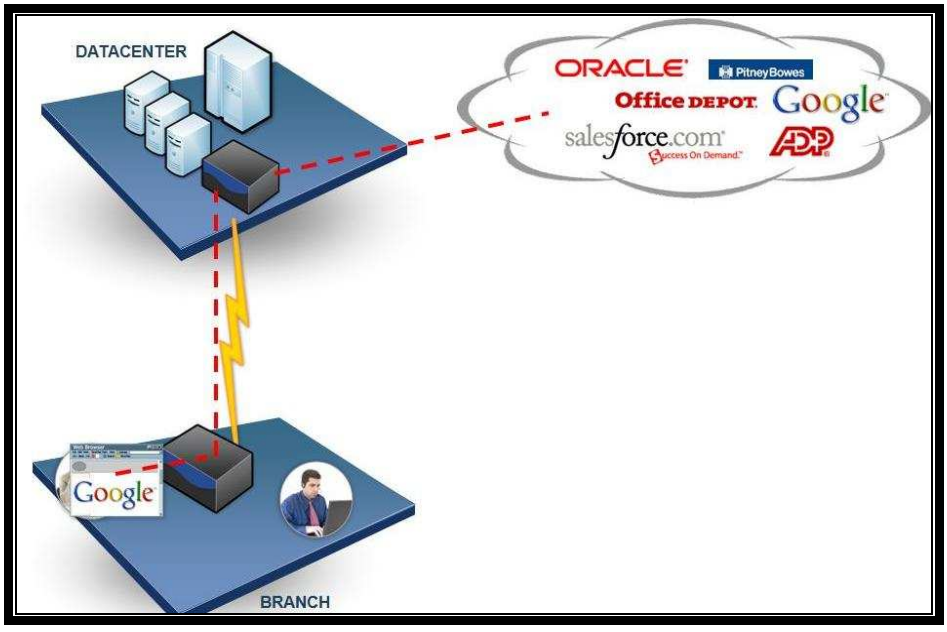


Figura 52 - Cache de Objetos.

5.8.4 Cache de Bytes

Tecnologia patenteada pela Blue Coat para elevar a eficiência reduzindo os dados transmitidos que se baseia na repetição de partes de um arquivo independente da

aplicação envolvida. Estas partes seriam representadas por um token (chave) que atravessaria o link WAN e seria remontado no receptor.

O cache de Bytes representa muitos Megabytes de dados em apenas poucos bytes. Um token de poucos bytes pode representar um bloco de 64 kbytes.

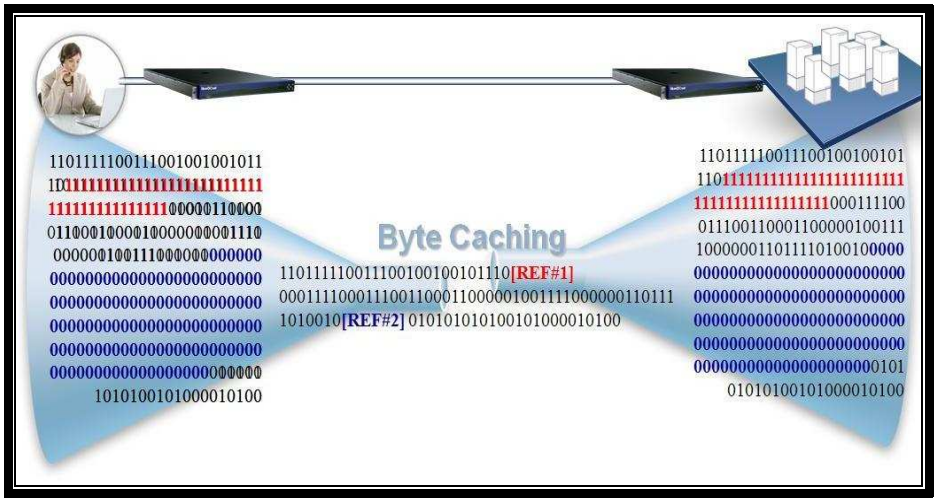


Figura 53 - Cache de Bytes.

5.8.5 Compressão

É aplicado um algoritmo para remover informações previsíveis e desnecessárias do trafego antes de ser enviado pelo link WAN. A informação é reconstruída ao chegar à outra ponta do link WAN utilizando o mesmo algoritmo (normalmente Gzip).

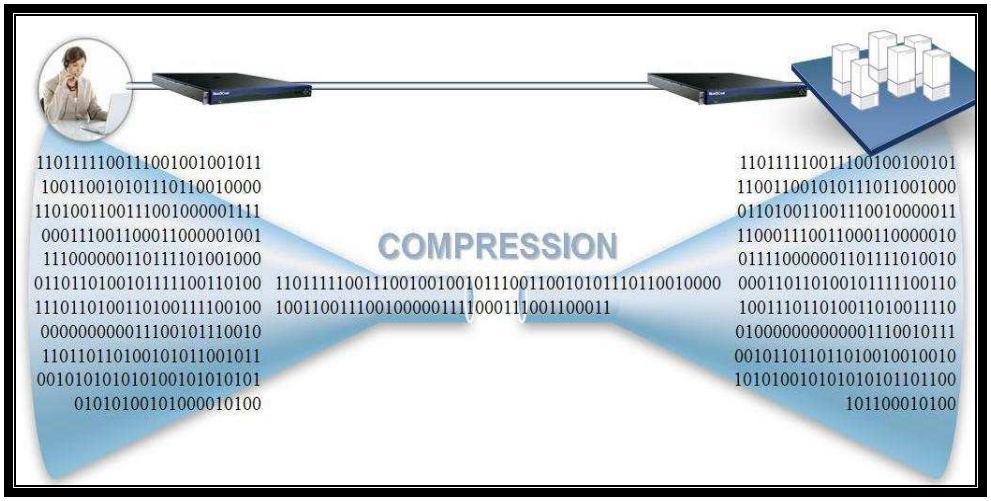


Figura 54 - Compressão do Trafego.

5.8.6 SG Client

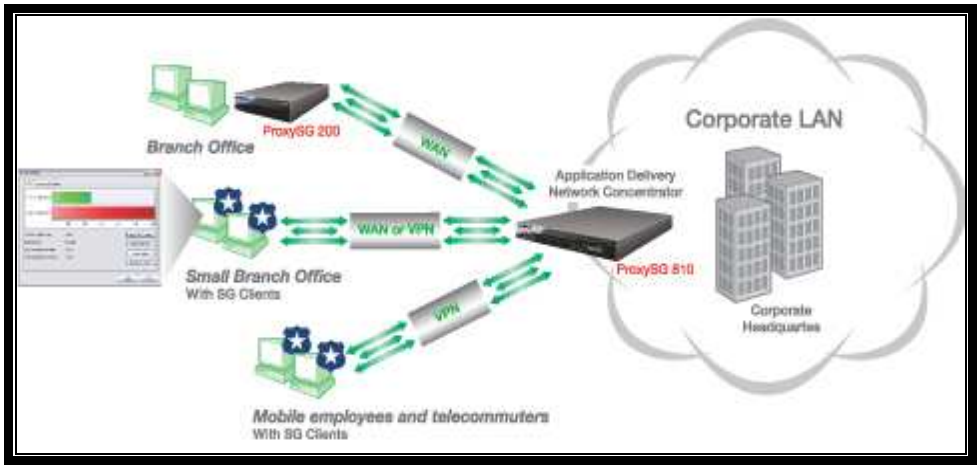


Figura 55 - Demonstrativo do uso do SG Client no ambiente corporativo.

A Blue Coat disponibiliza este Cliente para permitir que dispositivos móveis e filiais que estão fora da rede possam, através de VPN, se beneficiar das vantagens do MACH5.

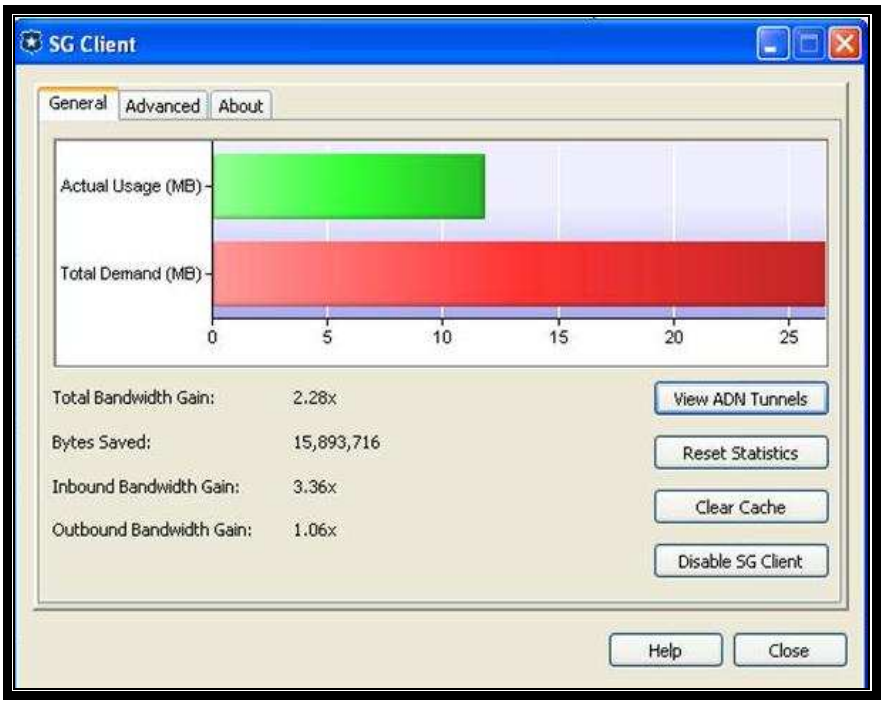


Figura 56 - Painel do SG Client.

Este ganho de desempenho e economia de link pode ser visto olhando o gráfico da figura 57, quando um arquivo é aberto pela primeira vez e quando é aberto pela segunda vez.

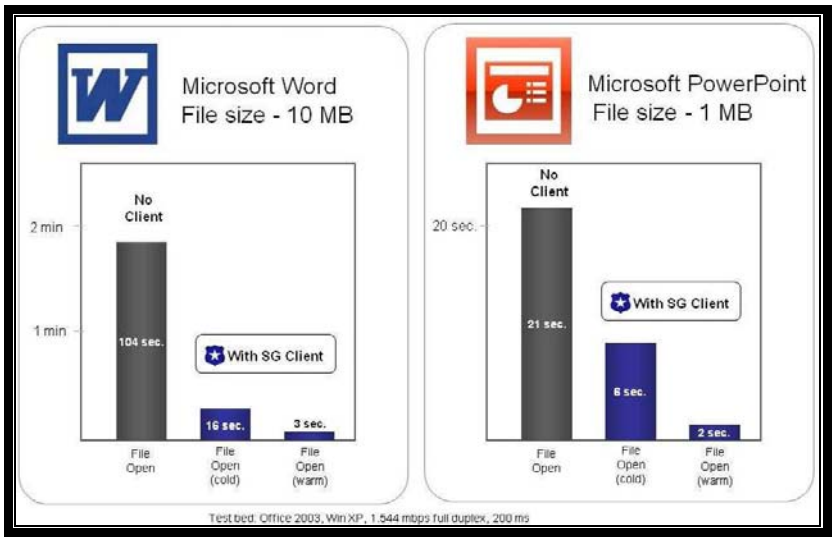


Figura 57 - Comparativo do uso do SG Client em documentos Office.

5.9 BLUE COAT REPORTER

O Blue Coat Reporter (versão Windows ou Linux) permite ao administrador da rede obter informações sobre a efetividade das políticas de segurança implementadas na rede, identificando possíveis falhas de segurança antes que haja impacto nos negócios.

É possível visualizar atividades dos usuários na rede, criar relatórios de tráfego por usuário, por tipo de arquivos, categorias, URLs e gerenciar recursos da rede identificando abusos de utilização da banda.

- O programa Reporter se encontra instalado em um servidor à parte com acesso através de FTP com o Proxy SG;
- Alguns requerimentos de hardware deverão ser considerados;
- Proxy SG pode ser configurado para mandar logs, funcionando como um cliente FTP, para um servidor FTP em tempo real ou não (via FTPS) que se localiza na maquina onde se encontra o Reporter;
- No Proxy SG não é possível a visualização de relatórios, apenas dos raw logs(logs não processados);
- Existem mais de 150 tipos de relatórios.

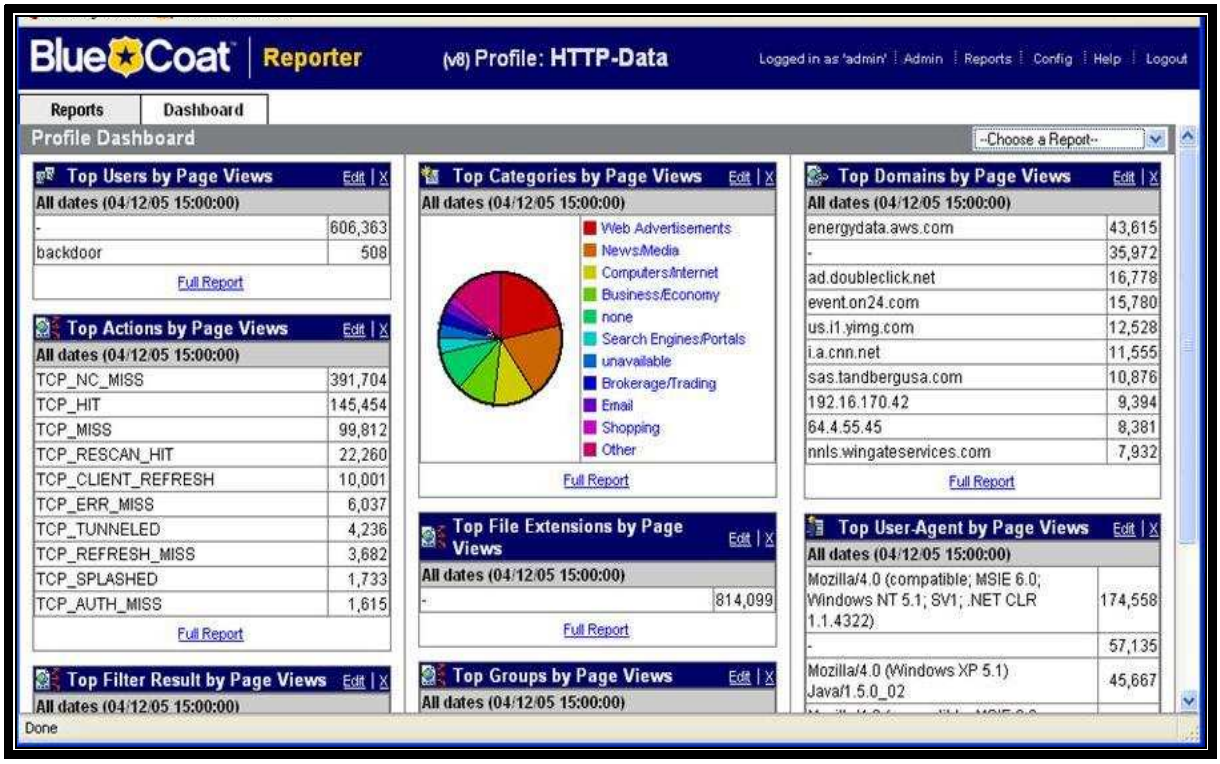


Figura 58 - Dashboard (Tela Principal do Blue Coat Reporter).

5.10 BLUE COAT DIRECTOR

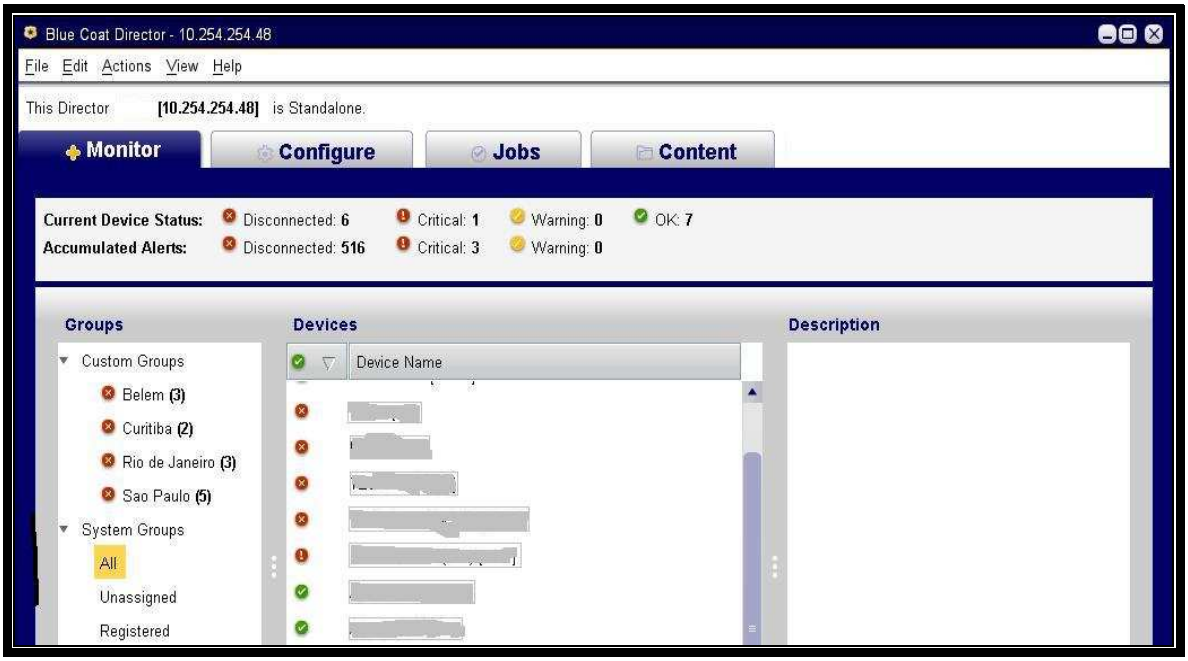


Figura 59 - Tela principal(Java) do Blue Coat Director.

O Blue Coat Director é destinado a automatizar e centralizar a mudança das políticas e configurações em uma rede distribuída de equipamentos Blue Coat. Isto permite que as empresas mantenham as mesmas políticas e configurações em todos os equipamentos. Há também a possibilidade da criação de grupos personalizados, por localidade ou ainda por grupo lógico de Blue Coats. Novas políticas podem ser criadas e instaladas nos equipamentos da rede em minutos sem que seja necessário qualquer tipo de configuração local.

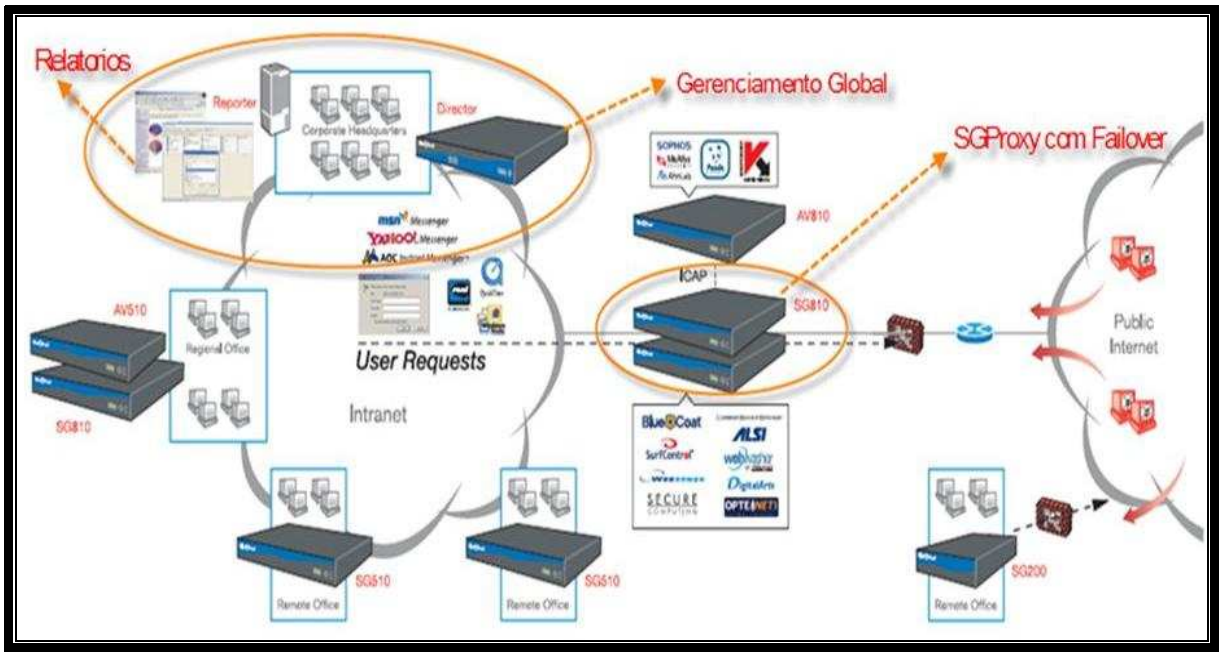


Figura 60 - Ambiente Blue Coat sendo utilizado para gerenciamento o Director.

6 TESTES DE CACHE COM SITE DE CONTEÚDO DINÂMICO

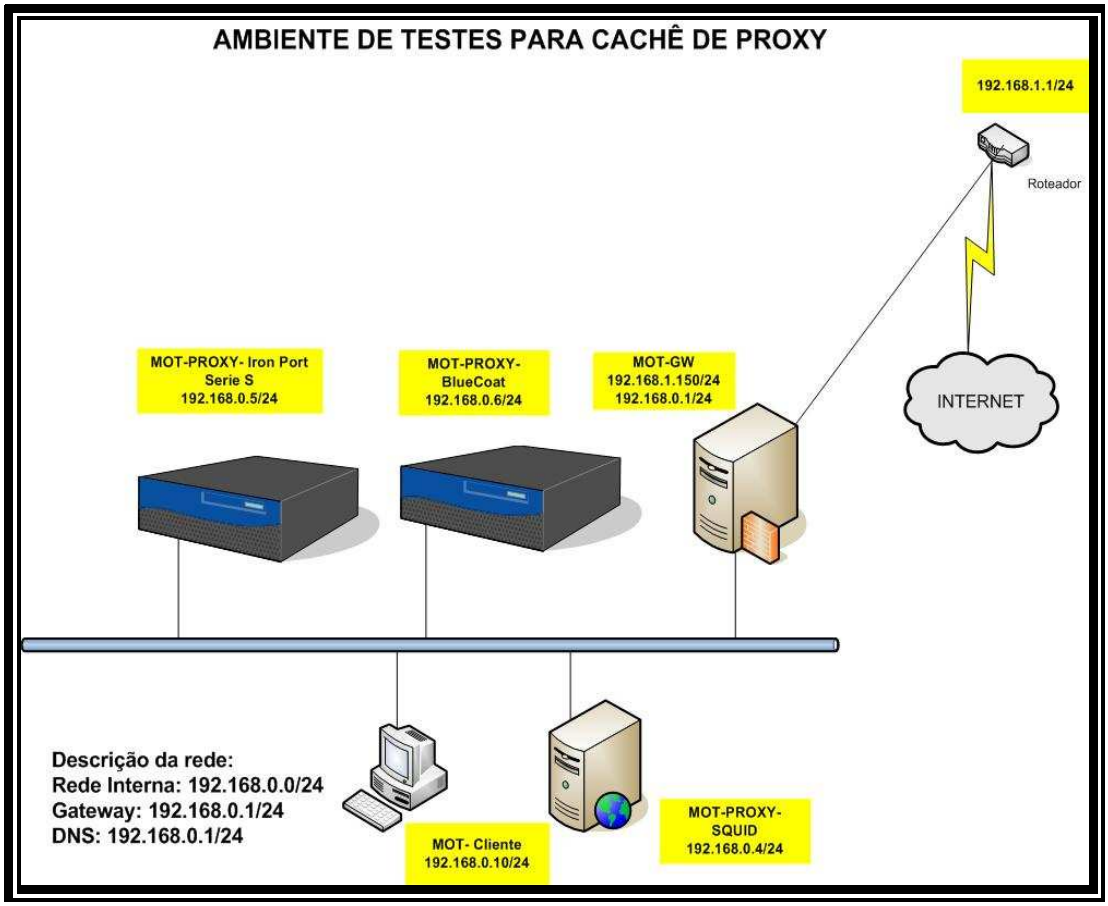


Figura 61 - Topologia do Ambiente de Testes

Através da ferramenta Wget (http://www.gnu.org/software/wget/) que foi preparada para utilizar a conexão através de Proxy, fez-se o download do índex.html principal do site WWW.uol.com.br (escolhido este devido ao alto nível de modificações feitas na pagina principal por dia/hora/minuto). O download foi realizado por canais diferentes. Primeiro diretamente pelo Firewall (sem intermediários além da própria Internet). Depois por três Proxies diferentes (Squid, Ironport Serie S e Blue Coat).

Configuração para uso de Proxy no Wget:

Para utilizar o Wget via Proxy (numa rede corporativa por exemplo), foi criado em seu $home o arquivo .wgetrc com o seguinte conteúdo:

```
proxy_passwd = sua_senha
http_proxy = http://IP:porta
proxy_user = seu_usuário
```

Com esta operação passou-se a ter quatro versões do índex.html da UOL salvos em diretórios separados. Após o download foi gerado um hash md5 de cada um e comparado com o arquivo baixado pelo Firewall (Gateway da Rede), pois este último está sempre mais atualizado com relação ao site naquele momento. Essa operação foi repetida a cada 5 minutos por um total de 60 minutos, de maneira que foi possível verificar qual dos Proxies entrega a página dinâmica mais atualizada mesmo estando em cache. Com todos os aparelhos foram utilizados com a configuração padrão de fábrica, o resultado pode ser alterado ao serem feitos os devidos ajustes em cada um. Foi marcado em negrito quando o hash de cada índex.html baixado pelo Proxy foi idêntico ao baixado pelo Firewall (Gateway).

6.1 - DIRETO DO GATEWAY (SEM INTERMEDIÁRIOS)

6.1.1 - Coleta de Dados

Será mostrado apenas a primeira coleta para fim ilustrativo, foram feitas 13 coletas, uma a cada 5 minutos.

```
root@mot-cliente:~# wget -r -A "index.html" -P Firewall/1/  http://www.uol.com.br
--2009-06-07 14:09:30--  http://www.uol.com.br/
Resolving www.uol.com.br... 200.221.2.45, 200.98.249.120
Connecting to www.uol.com.br|200.221.2.45|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: `Firewall/1/www.uol.com.br/index.html'
2009-06-07 14:09:30 (599 KB/s) - `Firewall/1/www.uol.com.br/index.html' saved [204636]
FINISHED --2009-06-07 14:09:30--
Downloaded: 1 files, 200K in 0,3s (599 KB/s)
```

6.1.2 - Extração do Hash do index.html

root@mot-cliente:~/Firewall/1/www.uol.com.br# md5sum index.html
d7eb55d12cc194110089f1906b47028a index.html <-- Inicio
d707c0bc26d5e286529922662b64dc39 index.html <-- 5 minutos após o inicio.
95341377d36f57a13190263220a35957 index.html <-- 10 minutos após o inicio.
c5591dd3cd56b10205eb3e922c9a6bd9 index.html <-- 15 minutos após o inicio.
421635f902075dba7096a3263a23d3df index.html <-- 20 minutos após o inicio.
5f1b2014039f159ba7e58a0564106424 index.html <-- 25 minutos após o inicio.
4a6763c087f4f74766e1c86e65de6b7c index.html <-- 30 minutos após o inicio.
349b304bc26e02b9043eaef0cd733e86 index.html <-- 35 minutos após o inicio.
12f7e0ad754cc98ade3356750aa1b682 index.html <-- 40 minutos após o inicio.
db41fa3e06c8e1ca5d3327d7652462a7 index.html <-- 45 minutos após o inicio.
38b39b149be743dff032c295a547efbb index.html <-- 50 minutos após o inicio.
96a2054887b3405a9de07312928696c4 index.html <-- 55 minutos após o inicio.
bcb57e9c6b1c7d4abff99ff5a7d24072 index.html <-- 60 minutos após o inicio.

6.2 - PROXY SQUID

6.2.1 - Coleta de Dados

Será mostrado apenas a primeira coleta para fim ilustrativo, foram feitas 13 coletas,

uma a cada 5 minutos.

root@mot-cliente:~# wget -r -A "index.html" -P Squid/1/ http://www.uol.com.br
--2009-06-07 14:09:45-- http://www.uol.com.br/
Connecting to **192.168.0.4:3128**... connected.
Proxy request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: `Squid/1/www.uol.com.br/index.html'
2009-06-07 14:09:45 (560 KB/s) - `Squid/1/www.uol.com.br/index.html' saved [205731]
FINISHED --2009-06-07 14:09:45--
Downloaded: 1 files, 201K in 0,4s (560 KB/s)

6.2.2 - Extração do Hash do index.html

root@mot-cliente:~/Squid/1/www.uol.com.br# md5sum index.html
d7eb55d12cc194110089f1906b47028a index.html <-- Inicio.
d7eb55d12cc194110089f1906b47028a index.html <-- 5 minutos após o inicio.
d7eb55d12cc194110089f1906b47028a index.html <-- 10 minutos após o inicio.
d7eb55d12cc194110089f1906b47028a index.html <-- 15 minutos após o inicio.
421635f902075dba7096a3263a23d3df index.html <-- 20 minutos após o inicio.
421635f902075dba7096a3263a23d3df index.html <-- 25 minutos após o inicio.
421635f902075dba7096a3263a23d3df index.html <-- 30 minutos após o inicio.
421635f902075dba7096a3263a23d3df index.html <-- 35 minutos após o inicio.
12f7e0ad754cc98ade3356750aa1b682 index.html <-- 40 minutos após o inicio.

12f7e0ad754cc98ade3356750aa1b682 index.html <-- 45 minutos após o inicio.
12f7e0ad754cc98ade3356750aa1b682 index.html <-- 50 minutos após o inicio.
12f7e0ad754cc98ade3356750aa1b682 index.html <-- 55 minutos após o inicio.
bcb57e9c6b1c7d4abff99ff5a7d24072 index.html <-- 60 minutos após o inicio.

6.3 - PROXY IRONPORT

6.3.1 - Coleta de Dados

Será mostrado apenas a primeira coleta para fim ilustrativo, foram feitas 13 coletas,

uma a cada 5 minutos.

root@mot-cliente:~# wget -r -A "index.html" -P Ironport/1/ http://www.uol.com.br
--2009-06-07 14:10:10-- http://www.uol.com.br/
Connecting to **192.168.0.5:8080**... connected.
Proxy request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: `Ironport/1/www.uol.com.br/index.html'
2009-06-07 14:10:10 (585 KB/s) - `Ironport/1/www.uol.com.br/index.html' saved [205433]
FINISHED --2009-06-07 14:10:10--
Downloaded: 1 files, 201K in 0,3s (585 KB/s)

6.3.2 - Extração do Hash do index.html

root@mot-cliente:~/Ironport/1/www.uol.com.br# md5sum index.html
d7eb55d12cc194110089f1906b47028a index.html <-- Inicio.
d7eb55d12cc194110089f1906b47028a index.html <-- 5 minutos após o inicio.
95341377d36f57a13190263220a35957 index.html <-- 10 minutos após o inicio.
c5591dd3cd56b10205eb3e922c9a6bd9 index.html <-- 15 minutos após o inicio.
421635f902075dba7096a3263a23d3df index.html <-- 20 minutos após o inicio.
421635f902075dba7096a3263a23d3df index.html <-- 20 minutos após o inicio.
4a6763c087f4f74766e1c86e65de6b7c index.html <-- 30 minutos após o inicio.
349b304bc26e02b9043eaef0cd733e86 index.html <-- 35 minutos após o inicio.
12f7e0ad754cc98ade3356750aa1b682 index.html <-- 40 minutos após o inicio.
12f7e0ad754cc98ade3356750aa1b682 index.html <-- 45 minutos após o inicio.
38b39b149be743dff032c295a547efbb index.html <-- 50 minutos após o inicio.
96a2054887b3405a9de07312928696c4 index.html <-- 55 minutos após o inicio.
bcb57e9c6b1c7d4abff99ff5a7d24072 index.html <-- 60 minutos após o inicio.

6.4 - PROXY BLUE COAT

6.4.1 - Coleta de Dados

Será mostrado apenas a primeira coleta para fim ilustrativo, foram feitas 13 coletas, uma a cada 5 minutos.

root@mot-cliente:~# wget -r -A "index.html" -P Bluecoat/1/ http://www.uol.com.br
--2009-06-07 14:09:58-- http://www.uol.com.br/
Connecting to **192.168.0.6:8080**... connected.
Proxy request sent, awaiting response... 200 OK
C [text/html]
Saving to: `Bluecoat/1/www.uol.com.br/index.html'
2009-06-07 14:09:58 (623 KB/s) - `Bluecoat/1/www.uol.com.br/index.html' saved [205354]
FINISHED --2009-06-07 14:09:58--
Downloaded: 1 files, 201K in 0,3s (623 KB/s)

6.4.2 - Extração do Hash do index.html

root@mot-cliente:~/Bluecoat/1/www.uol.com.br# md5sum index.html
d7eb55d12cc194110089f1906b47028a index.html <-- Inicio.
d707c0bc26d5e286529922662b64dc39 index.html <-- 5 Minutos Depois
95341377d36f57a13190263220a35957 index.html <-- 10 minutos após o inicio.
c5591dd3cd56b10205eb3e922c9a6bd9 index.html <-- 15 minutos após o inicio.
421635f902075dba7096a3263a23d3df index.html <-- 20 minutos após o inicio.
5f1b2014039f159ba7e58a0564106424 index.html <-- 25 minutos após o inicio.
5f1b2014039f159ba7e58a0564106424 index.html <-- 30 minutos após o inicio.
349b304bc26e02b9043eaef0cd733e86 index.html <-- 35 minutos após o inicio.
12f7e0ad754cc98ade3356750aa1b682 index.html <-- 40 minutos após o inicio.
db41fa3e06c8e1ca5d3327d7652462a7 index.html <-- 45 minutos após o inicio.
38b39b149be743dff032c295a547efbb index.html <-- 50 minutos após o inicio.
96a2054887b3405a9de07312928696c4 index.html <-- 55 minutos após o inicio.
96a2054887b3405a9de07312928696c4 index.html <-- 60 minutos após o inicio.

6.5 – ANALISE DOS RESULTADOS

Os resultados apresentados nos mostraram que o Blue Coat demonstrou um desempenho em seu cache superior aos outros equipamentos, apresentado um taxa de fornecer o conteúdo correto de 84,61%, contra 76,92% do Ironport e 30,76% do Squid. Isto é possível graças ao uso de sistema de arquivos proprietários e algoritmos de otimização de uso do cache utilizado nos Proxies proprietários,

permitindo que os clientes que acessam estes Proxies tenham sempre um conteúdo atualizado e desempenho na velocidade de carga do site, embora estejam se beneficiando diretamente do cache local.

Esta tecnologia também permite que seja feito o uso mais racional dos recursos disponíveis, mantendo a disponibilidade de banda no link de Internet para o serviço em si (HTTP e HTTPS), além de aumentar a possibilidade de garantia para outros serviços que fazem uso constante de link, como VOIP e outros.

7 CONCLUSÕES

Existe um abismo entre as funcionalidades e desempenho de Proxies proprietários e ferramentas de software livre. Conforme visto nas medições realizadas no capítulo 6, constataram-se que em configurações padrões de fábrica os Proxies proprietários possuem otimizações utilizando algoritmos que permitem o melhor aproveitamento do link WAN, cujo beneficio se torna mais evidente quando utilizado em larga escala.

Nestas medidas foi utilizado o site do provedor de conteúdo UOL (HTTP://www.uol.com.br) como referencia devido ao alto dinamismo das informações contidas nele. Quatro medidas foram tiradas em intervalos de 5 minutos cada: a primeira foi em uma conexão direta através do firewall e as outras três por intermédio do Proxy (e seu cache local), utilizamos três produtos diferentes (Squid, Ironport e Blue Coat) para avaliar seus desempenhos em entregar o conteúdo de forma mais otimizada (desempenho), porém mantendo o conteúdo minimamente defasado em relação ao conteúdo original do site durante aquele mesmo intervalo de tempo.

As ferramentas de software livre permitem que sejam customizadas para fazer grande parte das funcionalidades que são encontradas nos Proxies proprietários e também é possível melhorar o desempenho (levando em consideração hardware semelhante), com otimização do sistema de arquivos e pilhas de protocolos (redes e aplicações).

Porém, dispor de dinheiro em mão de obra especializada para investir nestas melhorias talvez não justifique o beneficio adquirido, uma vez que já existe a solução pronta. Cabe ao gestor avaliar se a compra de Proxies proprietários se justifica dentro da Analise/Avaliação de Riscos para o negocio da empresa, minimizando

impacto e probabilidade de uma ameaça explorar uma vulnerabilidade causando prejuízos de valores intangíveis (marca e imagem da empresa).

8 REFERÊNCIAS

[1] IRONPORT SYSTEMS INC. **AsyncOS 5.5 for WEB. IronPort S-Series Administration Version 2.1**

[2] IRONPORT SYSTEMS INC. **http://www.ironport.com** (acessado em março de 2008)

[3] BLUE COAT SYSTEMS INC. **Blue Coat Certified Proxy Administrator Course Version 2.0.2**

[4] BLUE COAT SYSTEMS INC. **Blue Coat Certified Proxy Professional Course Version 2.0.2**

[5] BLUE COAT SYSTEMS INC. **http://www.bluecoat.com** (acessado em março de 2008)

[6] WIKIPEDIA PROJECT. **http://en.wikipedia.org/wiki/Proxy_server** (acessado em maio de 2008)

[7] WIKIPEDIA PROJECT. **http://en.wikipedia.org/wiki/Squid_(software)** (acessado em maio de 2008)

[8] WIKIPEDIA PROJECT. **http://en.wikipedia.org/wiki/Blue_Coat_Systems** (acessado em maio de 2008)

[9] SQUID PROJECT. **http://www.squid-cache.org/** (acessado em março de 2008)